**Human user authentication based on mouse dynamics: A feasibility study**

by

Xuantong Zhang

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Computer Engineering

Program of Study Committee:

Yong Guan, Major Professor

Daji Qiao

Wensheng Zhang

Iowa State University

Ames, Iowa

2015

## DEDICATION

I would like to dedicate this thesis to my mother Susheng Xu and my father Jiaxiang Zhang without whose unconditional moral and financial support I would not have been able to complete this work.

# TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

# ACKNOWLEDGEMENTS

I would like to thank my committee chair, Yong Guan, and my committee members Daji Qiao and Wensheng Zhang, for their guidance and support throughout the course of this research. I also would like to thank Dr. Smiley-Oyen and Yanlong Song for their help in the experiment design. Without their corporation I would not be able to finish the study.

In addition, I would also like to thank my friends, colleagues, the department faculty and staff for making my time at Iowa State University a wonderful experience. I want to also offer my appreciation to those who were willing to participate in my surveys and observations, without whom, this thesis would not have been possible.

# ABSTRACT

Security problems have been discussed for a long time in the past recent decades in many fields such as communication, networking and user authentication. Security and authentication methods have also been explored for a long time by many researchers, and many efficient ways have been developed and used in modern society. Password and fingerprint based user authentication methods are most common user authentication methods being used in our daily lives. With computers and smart phones population growing vastly, we need to put more attention on the security methods. However, those traditional authentication methods are not safe and efficient enough. Passwords are stolen and revealed to hackers, while fingerprint can be easily got from an authenticated person. We moved our eyes on another way of security and authentication- biometric kinesiology. The muscle in our body can remember the movement if we practiced an action a lot, and that memory is built in the body, not in our brain memory, which means that we cannot forget a practiced action in the way we forget a password. We proposed to use the action with mouse from an authenticated user as the password of a system, in which only the user perform right action can be regarded as an authenticated user. Otherwise the system will reject the user. This movement is hard to mimic unless the hacker do a lot of practice of that certain movement and do exactly the same as an authenticated user. This is very difficult because we modified the normal mouse and the mouse will not move as the hacker expect. What's more, only the authenticated user knows how was the mouse be modified and how to act to adjust to that modification. In this way our proposed approach is much safer than the above traditional security and authentication methods. However, this is a feasibility study and more experiment will be done to prove our proposal and we will discuss it in the future work chapter.

# CHAPTER 1. OVERVIEW

User authentication is very interesting in academia fields while it is also widely used in industrial fields. There are two kinds of user authentication generally the first kind of user authentication is to differentiate the authenticated user from other people. This kind of authentication is often used in the scenario where there is only single user for a device. For example, personal computer and mobile phone, such devices are often belong to one user, so the authentication method is focused on differentiating authenticated user from others. While in other scenarios that a device has many users to access, only tell the difference of a user from other people is not enough, the authentication method should be able to tell whether a person is an authenticated user or not, and besides that, the method should be able to tell who the authenticated user is among those users who are all authenticated. In those scenatios the second catrgory of user authentication is required. Such scenarios are also very common, for instance, the public computer in a university library. All the students in that university should be able to login to the computer system and the authentication method can tell which student the user is.

Authentication methods can be one-factor authentication or multi-factor authentication based on the number of factors can be used in the authentication process. Those authentication methods count on one factor such as face, speech, password is one factor authentication, while those based on two factors such as speech and facial recognition together is multi-factor authentication. Generally, multi-factor authentication methods are safer than one factor authentication methods. But the former ones are more difficult to implement and access. What's more, among those multi-factor user authentication methods, two-factor user authentication is more common.

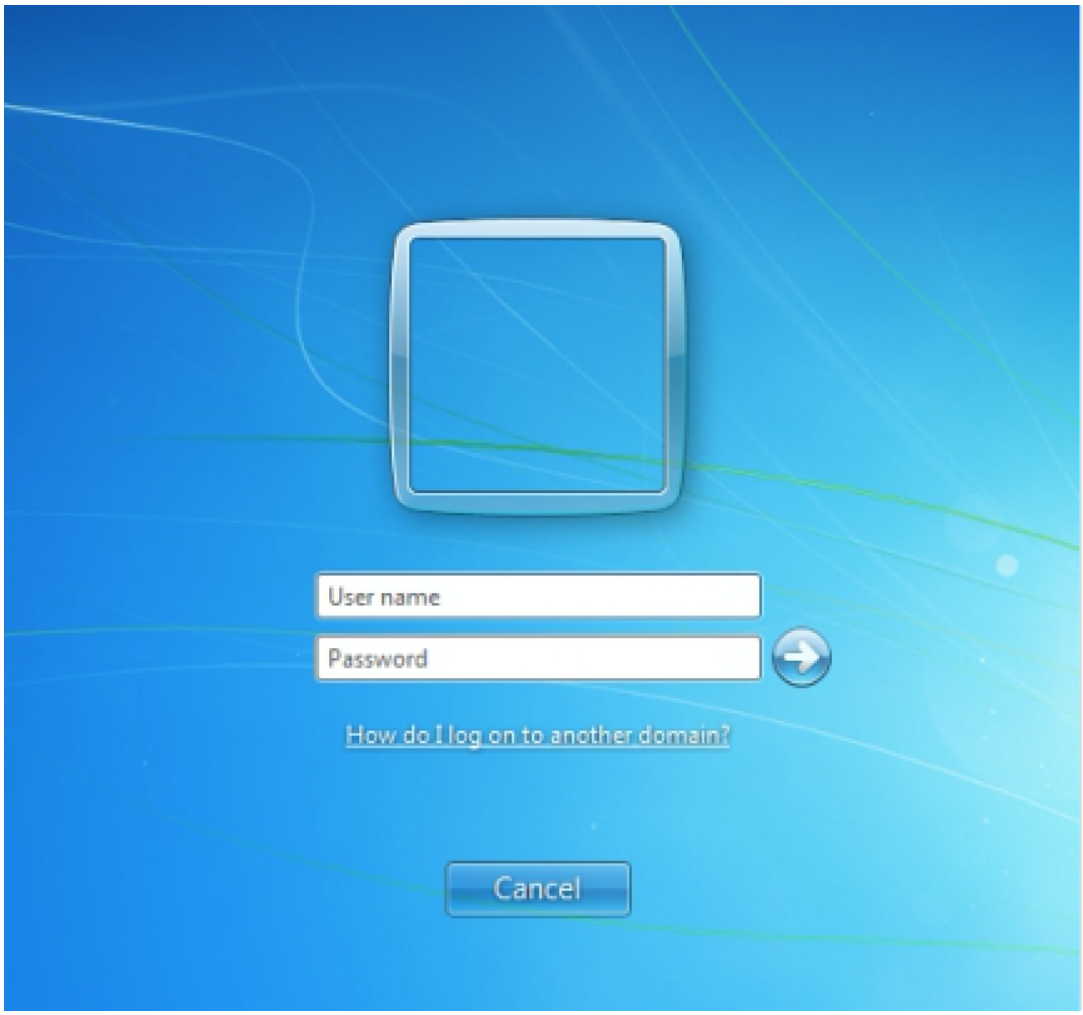



Figure 1.1 Popular computer and laptop login page

There are many categories of authentication methods when the classifying factor is the feature used in those methods but not the objective. Most people are familiar with some of the authentication methods in daily lives, such as password and username method, fingerprint method. There are also some methods people are not familiar with or has not been applied into industry but just remains in research level. In the following paragraphs details of some major authentication methods will be discussed.

## 1.1 Password Method

Passwords are widely used in modern daily life. When people use some web related applications it is usually required to create an account and to set username and password. The next time you want to login to your account you need to enter both your user name and password to access. This method seems to be very safe because others do not know what is your user name and password and you can make your password very complex and long, that people cannot guess your password. However, this widely used authentication method has many weaknesses in many aspects. The main weakness is that your password lies in the chain from your computer to the Internet. Internet will make password unsafe. A computer's system security usually relies on the login page, as we can see from Fig. 1.1. When a user try to login to a computer, he or she must enter the right username and password. This method seems to be the only access requirement of a computer. Once a hacker from the internet get your input byhacking then the security guard will be broken easily. Smart phones are in the similar situation. When you use a mobile phone, the most common login page still requires a password to enter by the user, shown in Fig. 1.2. But is it not really safe either. The other way for hackers to break in a computer is to use the brute force, which is easily to come up with, and, brute force often works. For both computers and smart phones, some of the login pages will show Invalid username' when you enter a wrong username. Then the hacker can find out what is the username and then try to find out the password. Certainly some system will give more generate information such as Invalid username or password', but this solution does not really help because the hacker can firstly enumerate the username then find out the password by brute force.

Besides the fact that password method itself is not really safe, many people in daily life they are using their passwords in a more dangerous way. The first mistake many people will make is that they would like to use pretty easy password such as '123456'. This kind of custom is very dangerous  hackers even do not need to hack, they can guess out the password. This is very dangerous but luckily more and more people are realizing it and are putting more attention on this issue. The second mistake usually seen in our lives is that people use a very complicated password, however, they use the same password everywhere needs a password. Once a password

has been stolen by a hacker, this hacker can easily access all other accounts. This kind of mistake happens because people cannot remember so many different passwords. In our life, basically everywhere you need to set up your password. In the bank, your finance issues are related to a password and you login to your Facebook account you also need a username and password. Email accounts, system in your university or company, they all require username and password. Clearly, with so many accounts to use everyday it is almost impossible for people to remember every password- if you want to set them all different and complex. The last mistake people tend to make is that when they use a public computer, their passwords are used to login to some system and the password will be exposed to the public. People lack the sense of security and privacy, so they just forget to logout or, some hackers can make use of the information put on the public machine. This is very dangerous especially when you put important messages, such as your SSN, bank account password, on the public computers. We are all exposed in the air.

Even if you are very careful about your password safe still you cannot be absolutely safe. Because the big companies you trust and give them your personal information but password will possibly be released by them. If you search password release you will find a lot of information about big companies related with such accidents. Your passwords are not safe even those companies have advanced security system.

## 1.2 Fingerprint Method

Fingerprints based authentication is another popular method for security and authentication use. This kind of methods differs from password methods in many ways. The first difference is that a person can create many passwords and change them if he or she likes. But people cannot have many fingerprints. We only have ten and we cannot change our fingerprints according to our preferences. The second way that fingerprint based authentication is different from password based authentication is that people cannot forget fingerprint, and they can just use them- they are on their hands. This sounds much better than password. A lot of movies and shows indicate that fingerprints are safer than passwords and such methods have been applied to the most important part of a system. However, although fingerprints are unique for every

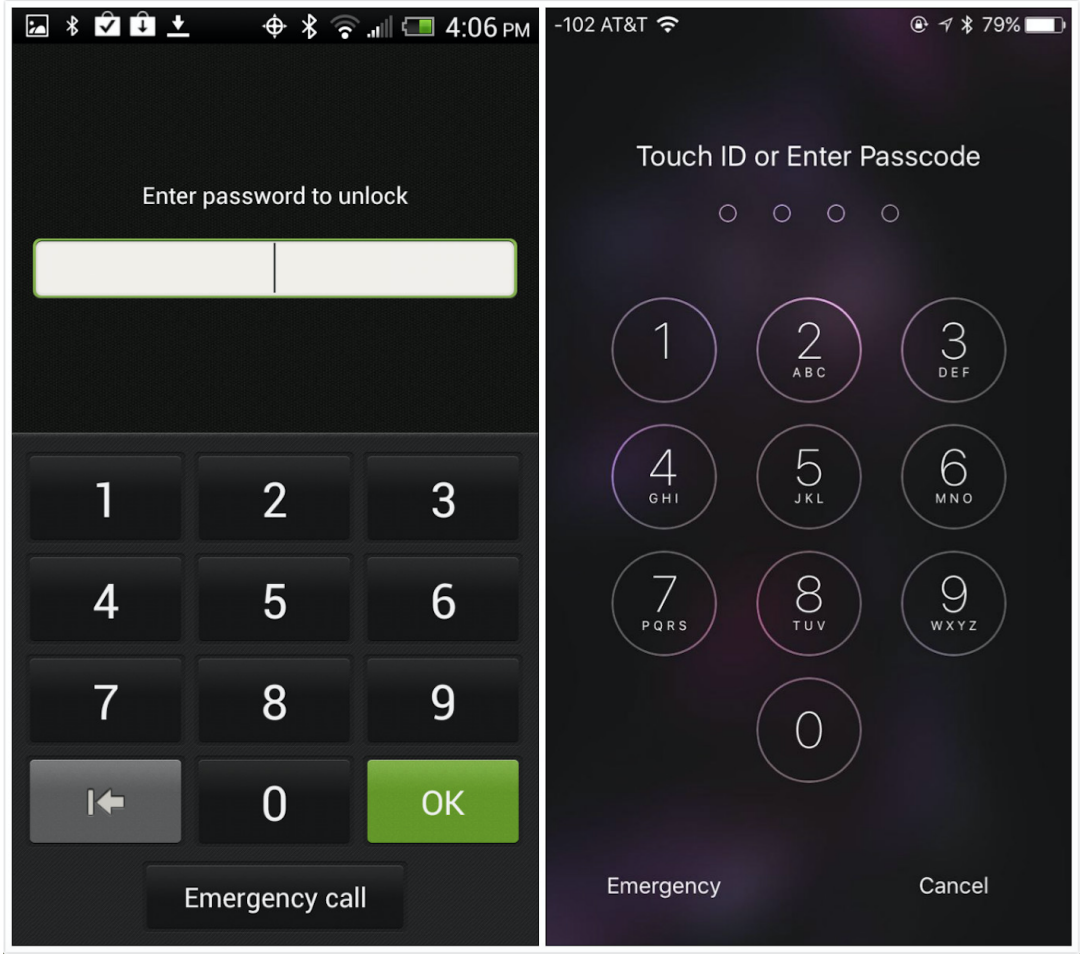



Figure 1.2 Popular smart phones login page with password and fingerprint login

person, fingerprint based authentication is not that safe and accurate. To make this clear, the first question is that how does the fingerprint based authentication work? How is the image of our fingerprints be compared and differentiated? The process is described the following: a picture of fingerprint needs to be taken, and once the picture is stored in a picture, the picture needs to be converted to a set of features which are the extractions from that fingerprint. These features will be stored in a template. Every time a user try to access the fingerprint security system, after taking the fingerprint and extracting the features, the features will be compared with the template. If the set of features and the template achieve high similarity according to some standard, the two finger will be considered match. But the above processes are not safe. The hackers can get the user's fingerprint to access the machine just by using it's owner's fingerprint. Especially for those who are familiar with the authenticated user, fingerprint is everywhere, and it's very easy for people to obtain a fingerprint. Even no hack techniques are needed and a person without any technical background can do in this way. From the above analysis we can know that the traditional and popular security methods are not safe from some aspects. The most disadvantages lies in that the authenticated or unique metric show the user's identity can be forgotten or stolen. Those aspects show our study has advantages over the traditional authentication work.

## 1.3 Facial Recognition Method

Facial recognition is not unfamiliar for people recently. Facial recognition can be used as user authentication obviously, and there are already many mature facial recognition software have been used in business. The famous one of those software is named Face++. The accuracy rate of such software is relatively high, however, if the hack uses a picture of authenticated user the software will recognize the hacker as authenticated user. This is very unsafe for secure use. Moreover, if the situation is dark and the camera cannot get the user's picture clearly, it is probable that the recognition is failed. Thus the authentication method has it's limitation while it is really convenient to use.

## 1.4 Other Authentication Methods

There are still many other researches on user authentications based on other factors. For example, voice, typing stroke, veins and mouse dynamics are all can be the factor used to authenticate users. Most of those works are still under research and has not been widely used in industry. However, like our approach, those authentication methods have advantages over the traditional authentication methods. Those works are worth researching and developing, and some of which are very promising. Details and examples of these works will be discussed in the literature survey chapter.

## 1.5 Advantage of Our Study

From the weakness of traditional authentication method we can see that it is relatively easy for hackers to break into system using those traditional authentication methods. There are three categories of authentication factors: something you have, something you know and something you are. Each factor in the authentication mechanism should be from a different category from the others [1]. Our objective is to test the feasibility of a special biometric, and see whether it can be used as the factor that only the users know and only they have, while others cannot get or steal from the users. We consider it should be some property lies in the user's body, like biometric metrics. A lot of similar work came out during last decades, showing the promising results of such authentication methods. Our study deals with the implementation and design of a series of experiment that will be used in the test of the feasibility of the proposed authentication method.

## 1.6 Organization of Thesis

The following chapters will be organized in this way: The second chapter will give literature survey and the information of former exploration of biometric metric used authentication. The third chapter will reveal information about the approach and objective of our research. The fourth chapter will give detailed information about experiment design and data collection methods. The last chapter is about the summary of our work and discussion of future work.

# CHAPTER 2. LITERATURE SURVEY

In the past decades many user authentication related researches have been published. Besides the well developed authentication methods such as password and username authentication, fingerprint authentication and facial recognition based user authentication, some new methods have also been explored and discussed a lot. Those works include mouse dynamics based authentication, handwriting based authentication, speech based authentication, keyboard stroke based authentication etc. The following two sections will discuss the related works and the rest two sections will give our objective of the study.

## 2.1 Biometrics based user authentication works

Biometric user authentication has evoked many researches from science and industry fields in the past ten years. Many biometric techniques have been researched and developed by scientists and developers. For example, fingerprint has been widely used in many aspects both in industry and people's lives. [2] Some other biometric techniques such as keyboard stroke, speech, mouse dynamics and handwriting have also been discussed a lot by researchers.

Keyboard stroke has been explored for over hundred years, the first study [3] was in 1907, there are already several authentication patents based on keyboard stroke. Keyboard stoke as a factor for user authentication has many advantages. Keyboard is similar to mouse in our study, which is widely used in lives and thus it's very easy to implement. What's more, it can be continuously used during the access to certain device. However, keystroke dynamics as factor for user authentication also has many disadvantages. The first disadvantage is that the accuracy is relatively low. The major dynamics discussed in those works are typing rhythm and force applied to the keys. But the rhythm is easily affected by fatigue, dis-

traction and other distractions. However, typing biometrics are worth researching, a lot of works [4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] have been published in the recent decades. Typing biometrics features has been discussed since 1990, most of which are focused on the rhythm and the dynamics of keyboard, and these two factors are considered the metrics for distinguishing authenticated users from others. After collecting data of a certain sentence or paragraph, the rhythm and dynamics are also collected for an authenticated user. When doing re-authentication, the system needs to compare those rhythm and dynamics in the user database. If the similarity rate is high above specified value the current user will be regarded as authenticated user. In a recently published research, typing dynamics has been discussed again and new development has been achieved according to the writer. In [17], some researchers argued that the keyboard stroke dynamics are very unstable compared to other stable biometrics such as face, fingerprints. Even more, there are also publications argue the accuracy of the existing keystroke dynamics based user authentication works. There is work in which users are authenticated using keystroke dynamics acquired when typing fixed alphabetic strings on a mobile phone keypad. The employed statistical classifier is able to perform user verification with an average equal error rate of about 13%. This work [18] was focused on mobile devices. While some researchers who are focused on computer and laptop keyboards have tested their approach on 154 individuals, achieving a false alarm rate of about 4% and an impostor pass rate of less than 0.01%. In [19], the results are very promising and exciting for unstable biometrics based user authentication works. The accuracy and new features have been discussed and the experiment result is promising. The typing biometrics are similar to mouse movement biometrics in some aspects. But in our study we have modified the mouse thus the unauthenticated user is even harder to learn and mimic the biometrics of authenticated users. Compared to the typing biometrics features mouse moving biometrics is more accurate and safe.

There are also some studies take advantages of the vein of people as the recognition factor in the authentication method. In some studies, finger vein is used as the factor. The approach needs to find the vein in person's hand with thermal infrared camera. After getting the pictures of the vein the image can be calculated as a person's hand database. The vein image is combined with the hand shape of that person to improve accuracy [18]. Some researches use finger vein

but not palm veins as the biometric factor. Those researchers argued that people have different finger vein patterns that differ from others.

Table 2.1 Comparison among major biometrics

| Biometric | Uniqueness | Feedback | Can be cheated | Accuracy |
|---|---|---|---|---|
| Fingerprint | Y | N | Y | High |
| Face | Y | N | Y | Middle |
| Speech | Y | N | Y | Middle |
| Handwriting | Y | N | Y | Middle |
| Vein | Y | N | N | Middle |
| Keyboard Stroke | Y | N | N | Middle |
| Mouse dynamics | Y | Y | N | Middle |

Table 2.1 shows brief information about the major biometrics used in user authentication. The uniqueness shows if the biometric is unique, as we can see, all biometrics can be considered as unique, because there are no identical people in the world, the biometrics from two persons can be similar but cannot be the same. So is mouse dynamics unique. The second factor is feedback, which means that if the biometric needs the person to give feedback when authenticating. For example, for fingerprint authentication, all the person has to do is to put his or her finger on the specific camera. So there is no feedback we can see from the person. It is similar for other biometrics except for mouse dynamics. This is because when you type on the keyboard, people do not need to look at the screen, but when moving the mouse, there is no way they don't look at the screen. People need to see the screen while they are moving the mouse, if the cursor is not in the direction it supposed to be, people can redirect the cursor, and the cursor's position is the feedback to people. Feedback is very important. If we give people different feedback, they will act differently, probably very differently. Thus we can see the differences among people more evidently. This is very important for our study. And this is also the keypoint in our study.

Besides those researches [20, 21, 22] based on single biometric feature, there are researches based on two or more biometric features, such as authentication method based on speech and handwriting [23]. Mouse dynamics biometrics has also been discussed a lot in the recent past years, the following paragraph will focus on the existing work related with mouse biometrics.

## 2.2 Mouse dynamics related work

Mouse is widely used in people's lives. Either touch board or mouse is needed for daily use of a computer. But mouse has been developed for nearly fifty years thus the functions are very complete and people are more familiar with it compared to touch board and touch screen. So although our idea can be applied to all these tools mentioned, we decided to make our first step with mouse. It is cheap and the APIs are very developed. As stated before, mouse biometrics has been discussed a lot in the past recent years. Some researchers researched on the features of mouse movement of a user and based on those features they developed database of that user. If another user's mouse movement data does not match the authenticated user then the user will be unauthenticated and rejected by the system. Some work has achieved very promising result. In this study [24], with huge amount of data collected the researchers argued that they have achieved a false acceptance rate (FAR) of 2.4649 percent and a false rejection rate (FRR) of 2.4614 percent. This result is exciting, however, there are only 22 subjects attending the experiments. Also, the researchers underlies that the hypothesis is that one can successfully model user behavior on the basis of user-invoked mouse movements. After they have collected the normal behavior of a user, when another user's actions deviates from the collected normal actions the current user will be judged as fraud. They claimed that their empirical results for eleven users show that they can differentiate these individuals based on their mouse movement behavior with a false positive rate of 0.43% and a false negative rate of 1.75% . This result is much better compared to another research group that uses the similar way but different settings [25]. Their research claimed that achieves a false-acceptance rate of 8.74%, and a false-rejection rate of 7.69% with a corresponding authentication time of 11.8 seconds. Mouse movement based works are basically in the same way. The differences of those works are the methods they used for extracting authenticated user's feature are different. However, some researchers doubt the experiment results of several existing work and does the experiments again to judge the experiment results claimed by those researches. In [26], there are survey papers about user authentication based on mouse dynamics [27, 28].

In the existing works the mouse have been used in the experiments are all normal mouse, which have no differences from the mouse people use in their computers. In our designed experiment, we modified the mouse cursor's position with an offset angle, making the mouse not acting normally'. Under such situation, the subjects will feel confused and they will try to learn to control the modified mouse. Before trying and learning, they cannot move the mouse as they want. Thus we can differentiate the authenticated user from others.

Our work will make the differences of behaviors of authenticated users and unauthenticated users more obvious and more different thus our approach can achieve more accurate result. We have mentioned that the feedback of people is the point we are interested and we believe that the feedback will make every person's differences from others clearer. In our study, we are trying to make the feedback behavior more clear to collect and analyze by adding an offset angle in the mouse. The details of the implementation will be described in the following chapters. However, our study is focused on feasibility, and we do not have enough data to get the fully convincing result. Which will be fulfilled in our future work.

# CHAPTER 3. OBJECTIVES OF THIS RESEARCH

## 3.1 System Design

The idea of user authentication with I/O devices such as mouse and touch screens has aroused much attention in the recent decade. Many approaches related have emerged with very positive experimental results. The objective of our research is to use our authentication approach on both laptop or computer and mobile devices with touch screen such as smart phones and tablets.

In this designed experiment, our device is a computer with Windows 7 system and a USB lined mouse. We implemented a user interface to collect the data and modify the offset angle of mouse. Thus our system is a computer, and laptop should be similar in this experiment. We use USB lined mouse because it is easier to implement then we can minimize the interferences.

Although our research is focused on computer with mouse, touch screen is similar with mouse approach that previous work has shown. Mobile devices authentication with motion dynamics has great value because of the population of mobile device growing larger and larger. Our future work will work on mobile devices with touch screen and users can unlock the screen with finger gestures.

People are familiar with mouse or finger touch in daily life on many devices due to the vast population of such devices. Many researchers work on such motion devices based authentication. However, people are so familiar to such devices so there is possibility that other unauthenticated people can mimic the movement of an authenticated user. We can believe from long time study and much practice such movement mimic can be achieved. So we intended to design a system that is hard to mimic or steal from authenticated users. Our experiments designed in the way that making the mouse movement unfamiliar to people and see if certain

changes have been made, whether we can recognize people according to the reaction people act to that change. Human beings' muscle can have a kind of memory, and the feedback goes according to those memories. Once a person learned a certain muscle movement, he or she will act the same in the same kind of behaviors. We can take advantage of this property in kinesiology to develop our experiment and thus build up our system. According to the feedback from the user being tested we can judge if he or she has been trained to adjust to the change. If not then we can decide this person is not an authenticated user.

## 3.2 Objective

Our objective of this research is to test the feasibility of our proposed approach- to see whether mouse dynamics can be used in single-user device(in this experiment, computer), if yes, we have plans for future work to improve our approach.

Our purpose is to distinguish the authenticated user from all other people. We will give the mouse in the login page an angle offset. Other people except the user have no knowledge about the angle offset, only the user is familiar with it. We will keep the user's data and the user should practice a lot before getting skilled about the mouse angle offset. From practicing people can learn to move more and more skillfully. But without practice, other people can't perform good especially they do not know what angle offset has been set.

Our objective is to test and explore whether this approach can be used for user re-authentication. Authentication based on mouse or motion gestures is safer than traditional authentication approach because biometrics cannot be forgotten, while passwords are often forgotten by users, but at least we need to prove that our work is able to differentiate authenticated users from other people. And biometrics cannot be stolen from a person, while password and fingerprints can be gathered in many ways. Biometrics is deeply planted in people's muscle and the reaction to certain muscle movement is natural and thus safe.

As for safety, we have mentioned in the above that this kind of property of human-beings is the muscle memory which is like feedback, when a movement is trained or practiced for a long time, a long-term muscle memory is created for that movement, and people will get used to the movement that such movement will not cost any effort to do. This process decreases

the need for attention and creates maximum efficiency within the motor and memory systems. Examples of muscle memory are found in many everyday activities that become automatic and improve with practice, such as riding a bicycle, typing on a keyboard, typing in a PIN, playing a musical instrument, or martial arts [29], and our experiment. Such muscle memories are hard to mimic when a unauthenticated user does not know what the certain change has been made to modify the mouse or touch screen. And this muscle memory cannot be stored in a hard drive thus cannot be stolen or replace.

In this research, the scenario we expect to implement the proposed approach is on single user devices. Which means our goal it to test if people have evident differences between the behaviors before practicing and after practicing. Before practicing, people are familiar with the normal mouse but cannot perform well with modified mouse. However, after certain amount of practicing(depends on the learning ability of a person), if the subject shows obvious improvement in the same task then we can say that the subject can learn from practice, thus we can differentiate other people from this subject. This is how we plan to implement our approach for user authentication. In real implementation, only the authenticated user knows how the device was modified and what was the angle. Even other people intended to mimic the movement they have no idea what the angle offset is and what the scale is. Therefore, this is convenient for user to access - the user does not need to remember any password, all they need is amount of practicing. If the approach works it is safe as we stated before.

After the entire research and experiment we will be able to answer below questions:

- Whether people can learn to adapt to modified mouse through practice.
- Does the amount of practice affect the learning process?
- What other factors can be taken into count that affects the learning process and data collection?
- How much practice does a subject need to do to be skilled in the experiment?
- Is our approach feasible?

In this study, because of the limitation of data collected we can only get the possible analysis. In the future work we will implement more experiments and make our results more accurate and we can answer those questions.

# CHAPTER 4. TWO IMPLEMENTATIONS OF MOUSE DYNAMICS BASED USER AUTHENTICATION

Our Approaches include two parts, and each part can perform the complete function of the designed system. One of our approaches is to implement the modification to mouse device in Linux kernel level. Since the modification lies in kernel level it will be hard for others to modify or break through, making the authentication method safer. Another approach is to build a graphical user interface from which we can collect data and perform the experiments conveniently. The reports and data will be collected and stored in a folder with user name and time. We can analyze those data collected from this application. What is more, with this user interface, people who take our experiments will not be distracted and can focus on the mouse movement itself. The following paragraphs will state the details of the two approaches.

## 4.1 Kernel Approach

Our kernel level approach is based on the Linux system. Linux operating system was first released in 1991, and it has been 24 years since its first version came out. Linux system is a Unix-like operating system which is free and open-source. The most important part of Linux operating system is Linux kernel. Linux kernel is primarily written in C and assembly language. Linux was originally developed as a free operating system for personal computers based on the Intel x86 architecture, but has since been ported to more computer hardware platforms than any other operating system. Many other operating systems like Android are built on the top of Linux kernel [30]. Which shows the vast population of Linux and related operating systems. Linux also run on embedded systems like car systems. From above, Linux system is a popular and stable system, and such property makes us choose Linux system as our system.

### 4.1.1 Linux kernel design

In a Unix-like system, processes are concurrent and they request system resources like network, memory. Linux kernel is a huge executable that handling all these requests by processes. Based on the function of kernel, Linux kernel can be split into five parts.

The first part is about processes management. This part is in charge of creating and destroying processes and deals with their communications to the user. In all operating systems such communications are based on signals, pipes and interprocess communications. This kind of function is acted by kernel. What is more, the scheduler is also controlled by kernel processes management.

The second functional part of Linux kernel is memory management part. This part of code deals with computer's memory, which is very important resource. Thus this part is very critical to the entire kernel. The kernel has virtual addressing space for processes on top of the limited available resources. In [31], the processes need to communicate with the memory management system through system calls.

The third part is file system. Like Unix, Linux is much based on the file system. We can treat everything in Linux system as a file system. The kernel is the organizer of the huge file system- it builds the file system on the hardware. This file system is an abstract file system, but it is very structured. Moreover, Linux supports multiple file systems thus we can have multiple ways to manage our files. The below chart shows more detailed information about Linux system design.

The next part is about device control. Almost very operating system finally make its operations reflect on hardware devices. Except for memory and processor and few other entities, any and all device control operations are performed by code that is specific to the device being addressed. That code is from the device drivers [31]. Mouse driver is one of them and we will discuss it in the following article because it is important to our mouse experiment kernel approach.

The last functional part is networking. Networking is also managed by operating system, because most networking operations are not specific to a certain process. The incoming packets

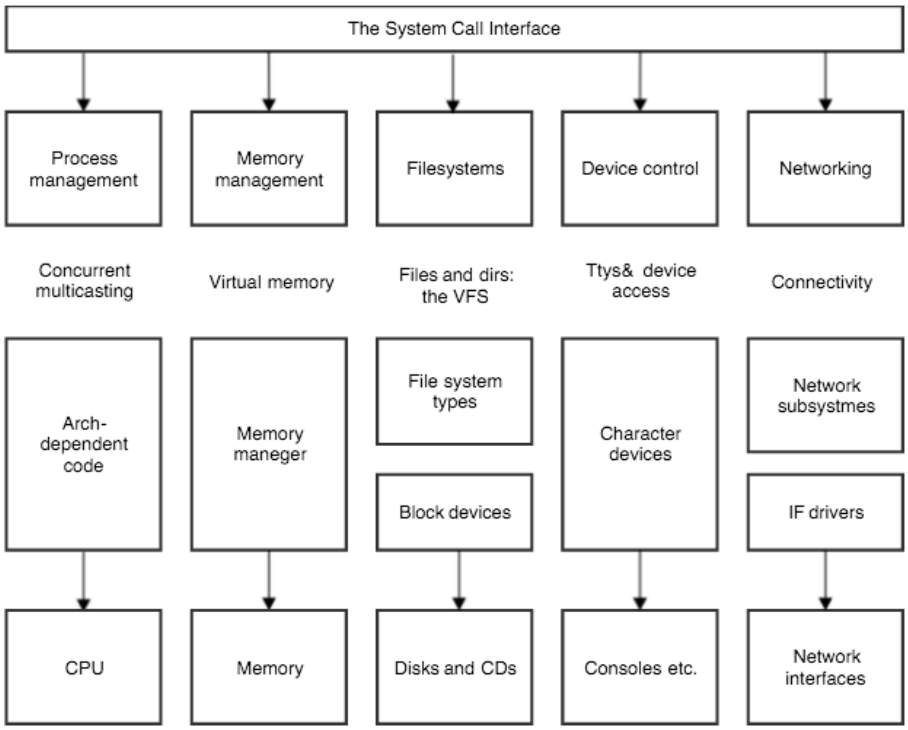



Figure 4.1 A split view of the kernel

must be collected and identified and then dispatched before a process can deal with them. Thus the system is in charge of sending the packets and receiving them. This part is not very related to our experiment design so I will not discuss more about it.

Table 4.1 shows the complete structure of kernel design and its relationship with user level design. By combining the functions stated above we can have a better understanding about Linux kernel. And we will focus on the device driver part of Linux kernel because this part contains the mouse driver, which contains the code we need to modify. Fig. 4.1 shows the split view of the Linux kernel.

### 4.1.2 Linux mouse driver modification

In our experiment design we need to modify the factors of mouse to change the mouse movement mode. Thus apparently we need to deal with mouse driver in our Linux approach.

Device driver is a very important part in Linux kernel, while it is very special. They act like a mysterious box to link the internal code with external devices and make them cooperate perfectly. They will not reveal the details about how the certain device is connected to the system calls but the user can do their activities with the device and the device driver. This kind of design makes the drivers can be a separate part from the other kernel codes and can be loaded whenever it is needed. The design indeed makes the device drivers can be relatively easy to write and modify when needed. Thus the mouse driver is a loadable module, which means that we can add or remove functions to kernel while the system is running. The added piece of code is called module. Not only device drivers but also other types can be modules that can be dynamically linked to the running kernel. With this property, we can modify the mouse driver and reload the module to make changes to the system.

## 4.2 User Interface Approach

To make the experiment environment more friendly and more accurate for data collecting we decided to create a user interface has the same function as our Linux kernel approach.

We created the user interface with Qt, an cross-platform application framework that is widely used for developing application software that can be run on various software and hardware platforms with little or no change in the underlying codebase, while having the power and speed of native applications. Because Qt [32] is an cross-platform application framework, our application can run on popular operation systems such as Linux, Windows and Mac OS. Qt is available with commercial and open source versions, we created our application using the open source version Qt5.5.

Table 4.1 Linux system design

| user mode | Low-level System components | System daemons | Windowing system | Other libraries | Graphics |
|---|---|---|---|---|---|
| ~~kernel mode~~ | System calls | | System calls interface | | |
| | Process scheduling | Memory Management | IPC | Virtual files system | Network subsystem |

Qt has many function modules which provide very complete functions for an application. Table 4.2 gives a brief introduction of Qt's modules and their function descriptions.

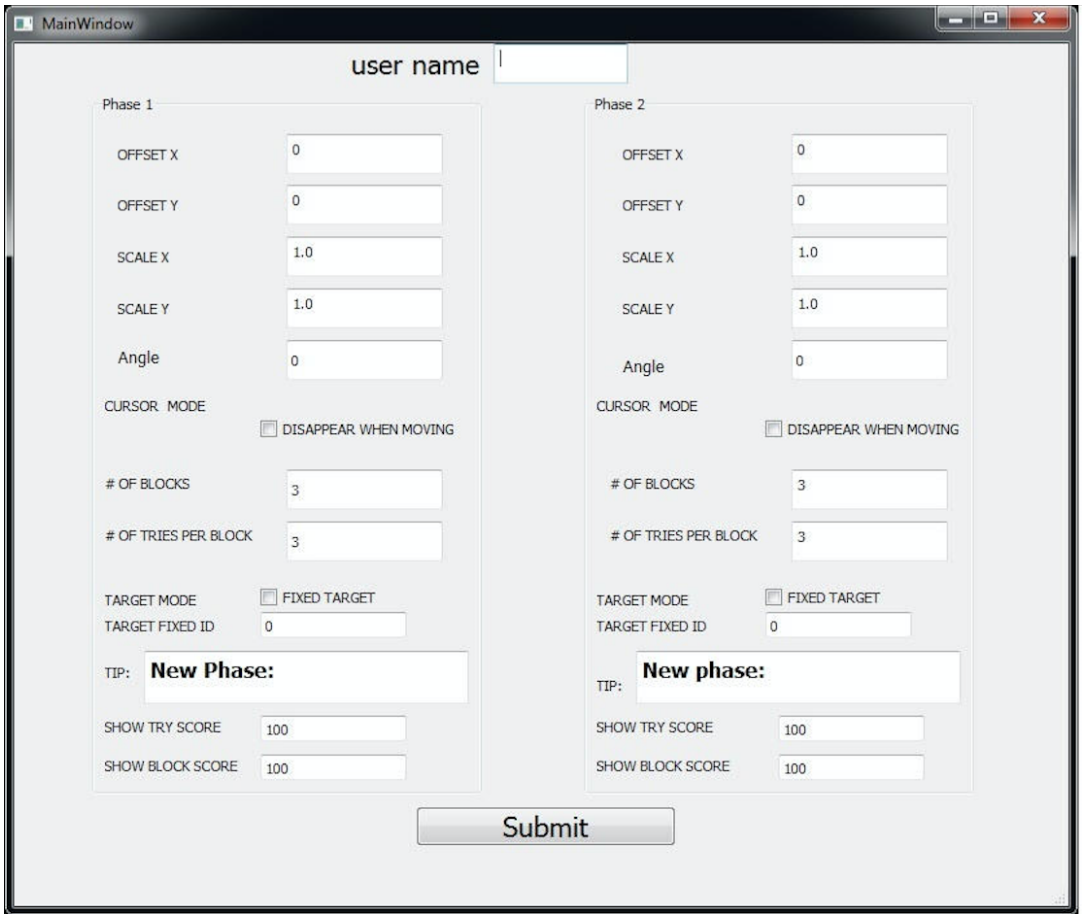



Figure 4.2 Phase settings

I created our experiment use application with Qt, and we did our experiments on a computer with Windows operating system. The following paragraph will give details about the user interface and experiment setup.

### 4.2.1 User interface details

For experimental use, the application we created is a perfect match for design of our experiment. The following will show details about the application. First, before we start experiment we need to set up the experiment environment. Our experiment is designed to have several phases, between phases there may have different factor settings. But in each phase the settings are the same. So our settings are designed to be filled in phase shown as Fig 4.2. In each trial

there is the start point and a target. The target can show up in 8 positions which are shown in Fig. 4.3.

Before set up an experiment for a subject we can enter the username of the subject thus the data will be recognized by different username. From Fig. 4.2 we can see that we can enter the OFFSET_X and OFFSET_Y values which will give a position offset each time the mouse position is collected by system. The frequency is 125 Hz. So each time the data is collected we change it to another position. We add an offset both on x-coordinate and y-coordinate. This is mode one. Mouse will change according to its current position. SCALE_X and SCALE_Y are similar with offset values, they calculate the difference of two continuous data collecting and times the difference by a number factor. So the scale factors are like speed factors. But because mouse positions are assessed according to the last position so these factors are complicated. For easier use and easier experiment, I have made the mouse tilt an angle from its original trace. The angle was calculated from the start point. This means that the mouse will not go to the direction the user let it go but tilt to another direction according to the angle we give it. The angle can be positive and negative, which is respectively clockwise and anticlockwise. In each trial, the subject needs to wait until the target turns green. From Fig. 4.4 we can see that before the target turning green it is red. And we can see from Fig. 4.5 when the target turns green means that the subject can move mouse toward the target.

There is a board circle which has the center located at the start point, and the radius is the distance from target to start position. When the cursor touches the board circle the trial will end. After the mouse hitting the board circle the last image showing where the mouse hit the mouse will freeze for two seconds to let the subject learn how did he or she moved the mouse. The subject will do the action according to the instruction given before each phase begins. To move slowly and precisely or to move very fast. the subject need to follow those instructions but not their preference. After each trail or block, we can decide whether to give the subject the score feedback or not the possibility. If we do not want to give the subject any score feedback, then we can set the possibility to 0. If after every trial in a phase we need to show the subject some feedback, like the score he or she has obtained, the time duration of last

Table 4.2 Qt Modules and functions

| Module | Description |
|---|---|
| **Qt Core** | The only required Qt module |
| **Qt GUI** | The central GUI module. |
| **Qt Widgets** | Contains classes for classic widget applications |
| **Qt QML** | Module forQMLandJavaScriptlanguages. |
| **Qt Quick** | The module for GUI application. |
| **Qt Quick Controls** | Widget like controls. |
| **Qt Quick Layouts** | Layouts for arranging items inQt Quick. |
| **Qt Network** | Network abstraction layer. |
| **Qt Multimedia** | Classes for audio, video, radio and camera functionality. |
| **Qt Multimedia Widgets** | The widgets fromQt Multimedia. |
| **Qt SQL** | Contains classes for database integration usingSQL. |
| **Qt WebKit** | Qt'sWebKitimplementation and API. |
| **Qt WebKit Widgets** | The widget API forQt WebKit |
| **Qt Test** | Classes for unit testing Qt applications and libraries. |

trail and the average distance from the ideal trace. Such data feedback is shown in Fig. 4.6, and I will explain about these factors in the data analysis chapter.

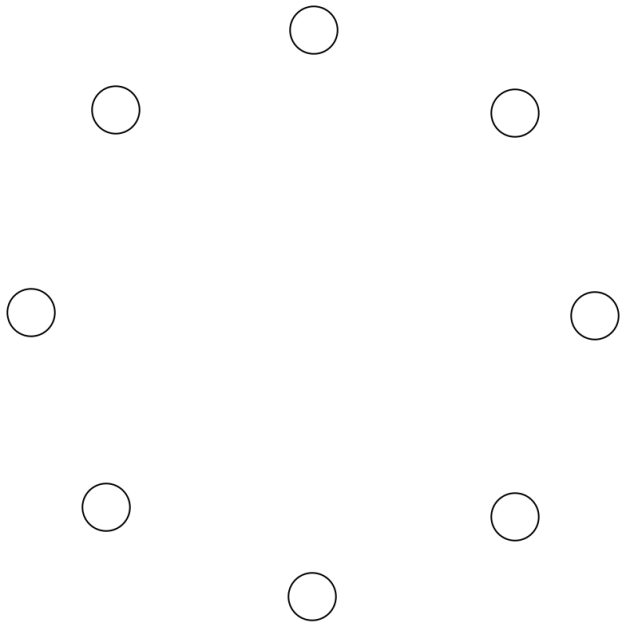


Figure 4.3 The positions of the targets

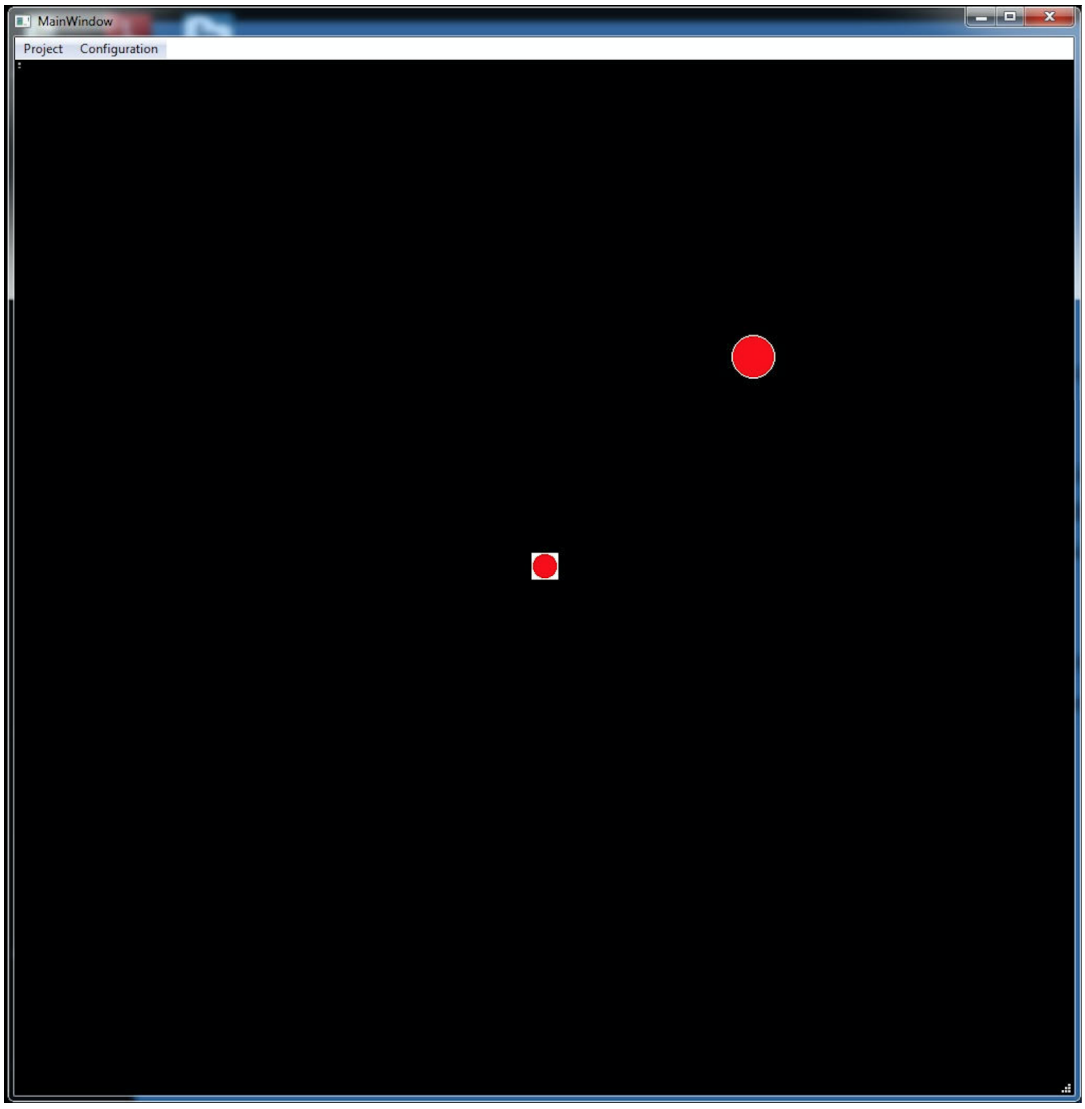



Figure 4.4 Target is red before starting trial

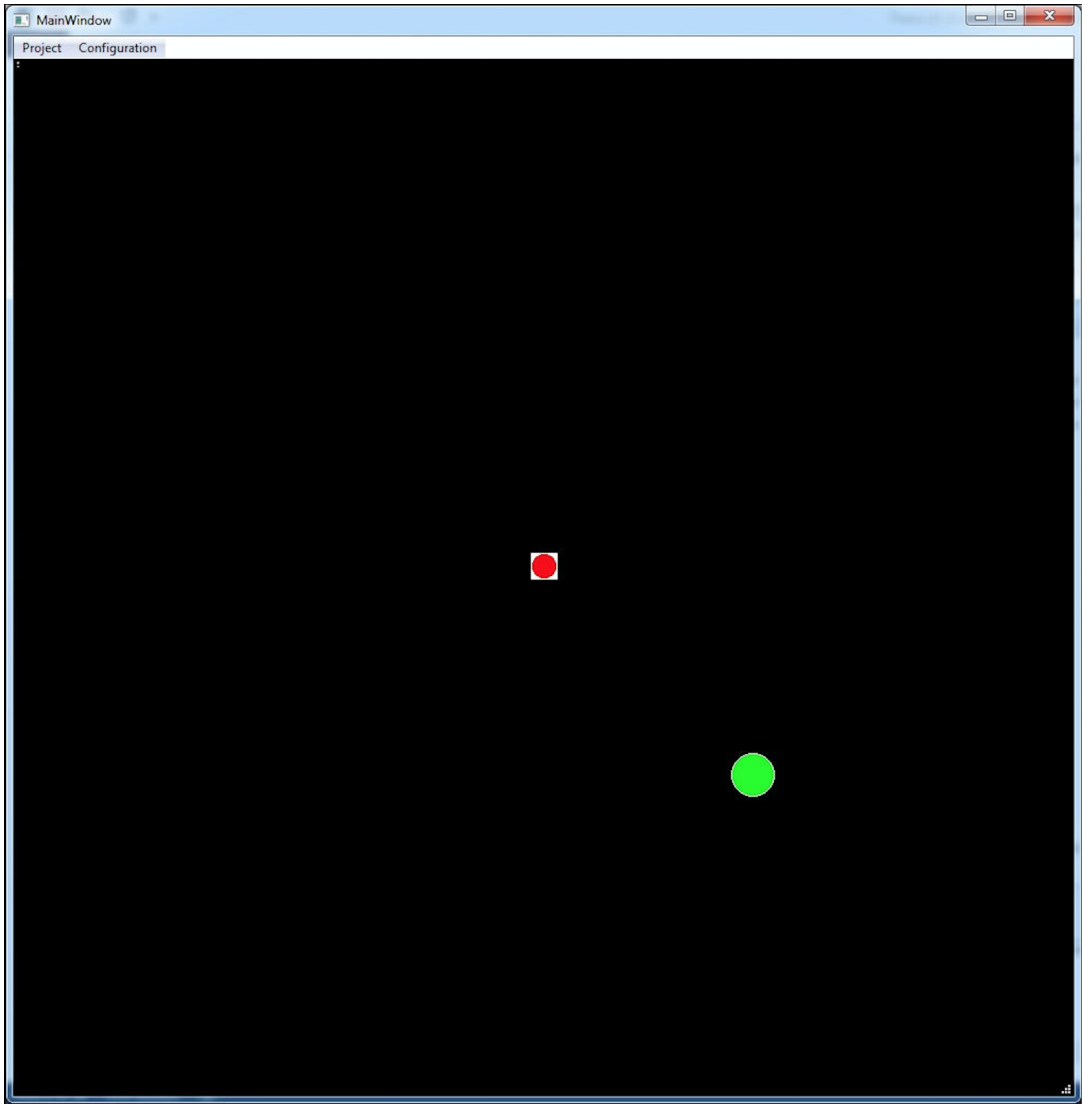



Figure 4.5 Target turns green when start


Figure 4.6 Feedback of trial and block

# CHAPTER 5. DATA COLLECTION

In this chapter we will discuss the experiment settings, data collection and our data analysis method.

## 5.1 Experiment Settings

The experiment settings were developed by our co-workers from Motor control & Learning Department of Kinesiology of Iowa State University. The complete experiment was composed of two sessions. The first session was developed for the subjects to study the mouse movement task and adjust themselves to the special mouse modification. We will see from their data that if the subjects have learned how to react to the modification of the mouse. And second session will happen after several days. If the subjects have learned how to adjust themselves to the new mouse, the second session will examine if they can still perform better than the original reaction. If they can we can say that such process and modification adjustment can be learned by people through much practice.

In the first session, there are 9 phases for each subject. The first two phases have no modification to the mouse, and the subject can get familiar with the environment and with the experimental task. After two phases, we start to introduce the angle tilt to the mouse, and the subject will first time experience the modified special mouse movement. Then after the third phase, we make the mouse back to the original normal mouse in the following two phases. In the next phase, the tilt angle comes to the mouse again with smaller angle and fixed target ID. The following phase will have random target to go further step to check if the subject has truly learned to adapt to modification. Then the next phase will make the angle bigger than before, to see if the angle get bigger and mouse get harder to control how will the subject adjust

to such change. Then the last phase will come back to the normal mouse, because we need to see after the learning process if the subject still can move the normal mouse without any interference, or the learning process has brought some memory into their normal stereotype of mouse moving.

Table 5.1 and Table 5.2 will show the details of each phase of the first session.

The second session is composed of seven phases. The second session are very similar to the first session but with the focus on practicing more. The details of second session settings are revealed by Table 5.3 and Table 5.4.

Table 5.1 Experiment setting for each phase (Session1-1)

| **Phase** | **# of Blocks** | **# of trials per block** | **Scale_X** | **Scale_Y** | **Angle** |
|---|---|---|---|---|---|
| **P1** | 1 | 10 | 1 | 1 | 0 |
| **P2** | 1 | 30 | 1 | 1 | 0 |
| **P3** | 1 | 30 | 1 | 1 | 25 |
| **P4** | 1 | 30 | 1 | 1 | 0 |
| **P5** | 1 | 30 | 1 | 1 | 0 |
| **P6** | 3 | 30 | 1 | 1 | 15 |
| **P7** | 4 | 30 | 1 | 1 | 15 |
| **P8** | 1 | 30 | 1 | 1 | 25 |
| **P9** | 1 | 30 | 1 | 1 | 0 |

Table 5.2 Experiment setting for each phase (Session1-2)

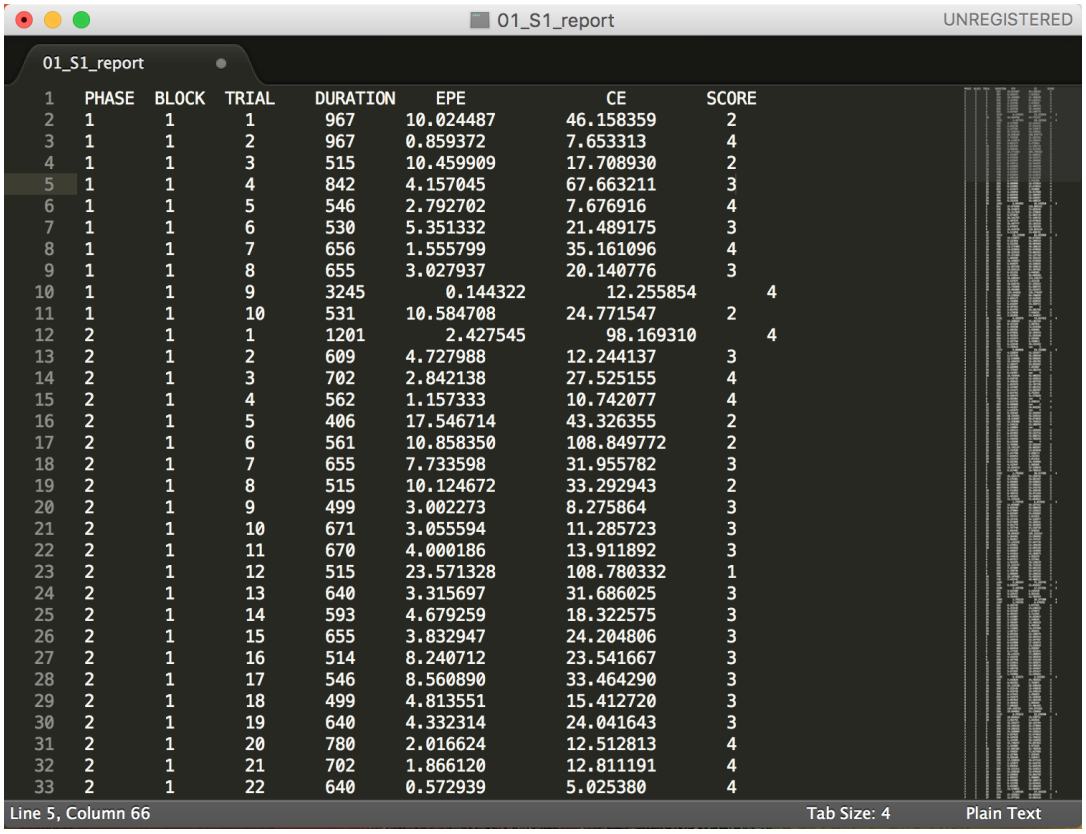
| **Phase** | **Target fixed** | **If fixed ID** | **Show cursor** | **Possibility of showing score** |
|---|---|---|---|---|
| **P1** | Y | 7 | Y | 100/100 |
| **P2** | N | N/A | Y | 100/100 |
| **P3** | N | N/A | Y | 100/100 |
| **P4** | Y | 7 | Y | 100/100 |
| **P5** | Y | 7 | Y | 100/100 |
| **P6** | Y | 7 | Y | 100/100 |
| **P7** | N | N/A | Y | 100/100 |
| **P8** | N | N/A | Y | 100/100 |
| **P9** | Y | 7 | Y | 100/100 |

Table 5.3 Experiment setting for each phase (Session2-1)

| | # of Blocks | # of trials per block | Scale_X | Scale_Y | Angle |
|---|---|---|---|---|---|
| **P1** | 1 | 30 | 1 | 1 | 15 |
| **P2** | 1 | 30 | 1 | 1 | 15 |
| **P3** | 4 | 30 | 1 | 1 | 15 |
| **P4** | 1 | 30 | 1 | 1 | 0 |
| **P5** | 1 | 30 | 1 | 1 | 0 |
| **P6** | 3 | 30 | 1 | 1 | 15 |
| **P7** | 1 | 30 | 1 | 1 | 25 |

Table 5.4 Experiment setting for each phase (Session2-2)

| | Target fixed | If fixed ID | Show cursor | Possibility of showing score |
|---|---|---|---|---|
| **P1** | Y | 7 | Y | 100/100 |
| **P2** | N | N/A | Y | 100/100 |
| **P3** | N | N/A | Y | 100/100 |
| **P4** | Y | 7 | Y | 100/100 |
| **P5** | Y | 7 | Y | 100/100 |
| **P6** | Y | 7 | Y | 100/100 |
| **P7** | N | N/A | Y | 100/100 |




| PHASE | BLOCK | TRIAL | DURATION | EPE | CE | SCORE |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 967 | 10.024487 | 46.158359 | 2 |
| 1 | 1 | 2 | 967 | 0.859372 | 7.653313 | 4 |
| 1 | 1 | 3 | 515 | 10.459909 | 17.708930 | 2 |
| 1 | 1 | 4 | 842 | 4.157045 | 67.663211 | 3 |
| 1 | 1 | 5 | 546 | 2.792702 | 7.676916 | 4 |
| 1 | 1 | 6 | 530 | 5.351332 | 21.489175 | 3 |
| 1 | 1 | 7 | 656 | 1.555799 | 35.161096 | 4 |
| 1 | 1 | 8 | 655 | 3.027937 | 20.140776 | 3 |
| 1 | 1 | 9 | 3245 | 0.144322 | 12.255854 | 4 |
| 1 | 1 | 10 | 531 | 10.584708 | 24.771547 | 2 |
| 2 | 1 | 1 | 1201 | 2.427545 | 98.169310 | 4 |
| 2 | 1 | 2 | 609 | 4.727988 | 12.244137 | 3 |
| 2 | 1 | 3 | 702 | 2.842138 | 27.525155 | 4 |
| 2 | 1 | 4 | 562 | 1.157333 | 10.742077 | 4 |
| 2 | 1 | 5 | 406 | 17.546714 | 43.326355 | 2 |
| 2 | 1 | 6 | 561 | 10.858350 | 108.849772 | 2 |
| 2 | 1 | 7 | 655 | 7.733598 | 31.955782 | 3 |
| 2 | 1 | 8 | 515 | 10.124672 | 33.292943 | 2 |
| 2 | 1 | 9 | 499 | 3.002273 | 8.275864 | 3 |
| 2 | 1 | 10 | 671 | 3.055594 | 11.285723 | 3 |
| 2 | 1 | 11 | 670 | 4.000186 | 13.911892 | 3 |
| 2 | 1 | 12 | 515 | 23.571328 | 108.780332 | 1 |
| 2 | 1 | 13 | 640 | 3.315697 | 31.686025 | 3 |
| 2 | 1 | 14 | 593 | 4.679259 | 18.322575 | 3 |
| 2 | 1 | 15 | 655 | 3.832947 | 24.204806 | 3 |
| 2 | 1 | 16 | 514 | 8.240712 | 23.541667 | 3 |
| 2 | 1 | 17 | 546 | 8.560890 | 33.464290 | 3 |
| 2 | 1 | 18 | 499 | 4.813551 | 15.412720 | 3 |
| 2 | 1 | 19 | 640 | 4.332314 | 24.041643 | 3 |
| 2 | 1 | 20 | 780 | 2.016624 | 12.512813 | 4 |
| 2 | 1 | 21 | 702 | 1.866120 | 12.811191 | 4 |
| 2 | 1 | 22 | 640 | 0.572939 | 5.025380 | 4 |

Figure 5.1 Sample report details

## 5.2 Data Analysis Method

The data analysis is focused on the factor data collected in the report. In the report we have details and factors we need. For instance we have collected the time duration of each trial with trial, block and phase number for each piece of data. Besides the time duration, we have EPE, which stands for end point error, showing when the subject moves the cursor out of boundary, the touching point is how many degrees tilt from the target. And we have CE, which stands for Cumulative error, shows the average distance of each trial. The distance calculation can be shown by Fig. 5.2. We also have score, the score is calculated by the equation given by Fig. 5.3. Fig. 5.1 is a sample report.

The score is calculated by the degree shown in Fig. 5.3, when the cursor touches the invisible boundary our system will collect the touching point and calculate the angle between two lines: one is the line from the start point to the touching point, the other line is also from the starting

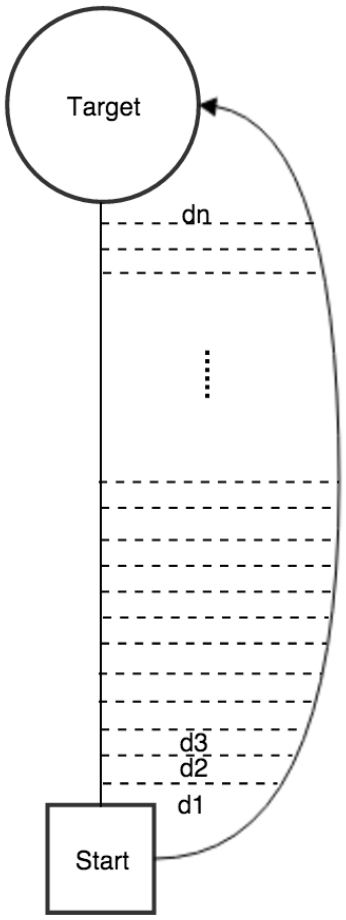



Figure 5.2 CE calculation distances

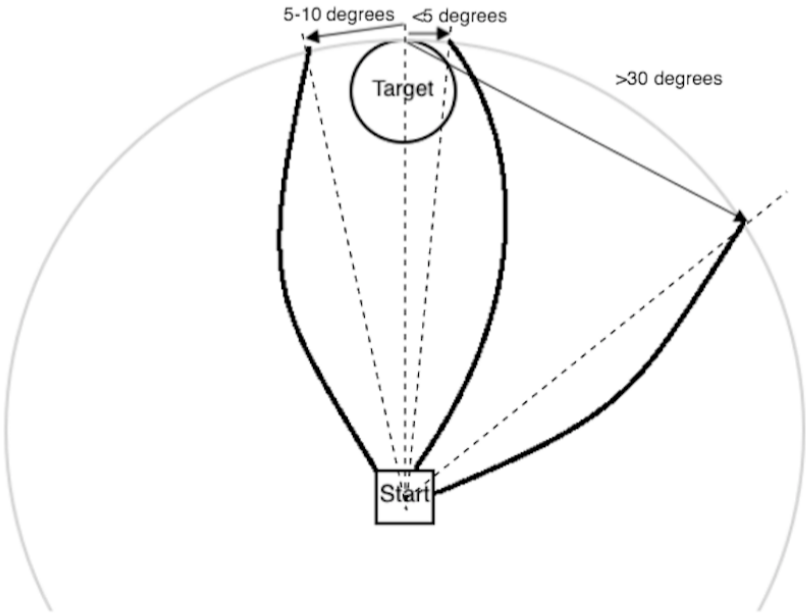



Figure 5.3 Score calculation details

point but end at the point the target touches the boundary. If the degree is less than 3, then we can regard it as the perfect move, we will give it a 4 (full score). If the angle is from 3 to 10 degrees, the score is 3, if 10-20 the score is 2, otherwise the score is 1.

The second level data analysis will give brief information about the certain factor in each block of a phase. We will analyze a factor, for instance the time duration of each trial in a block and plot them in a graph. From the graph we can easily figure out the tendency of that factor in that block and the tendency among phases if we compare the graphs in different phases. Other factors are also in the report, such as EPE, CE.

The third level data analysis is to give the changes among phases. We will compare the phases with same experiment settings, with one of them is before the practicing and the other is after the training. With such comparison we can see the differences of the subject's memory before and after practicing. And see if they can learn the process. One more thing is to compare the data figure of two phases, one phase is the first time practicing and second is the second

or third time practicing. With this we can learn the learning process, whether the subject can achieve better score when he or she practice more and more.

With the three phases we can get basically all the information we need to analyze our experiment process.

# CHAPTER 6. SUMMARY AND FUTURE WORK

## 6.1 Summary

In this designed experiment we focused on the learning process and testing the feasibility our proposed mouse dynamics based user authentication. We expect that people can learn from practice to adjust to the modified mouse, the more practice they do, the more skilled and accurate their performances are tend to be. We can possibly conclude that with a lot of practice people can perform certain mouse movement fluently and precisely. However, due to the time limit of our experiment, the data collected and the number of subjects both are very limited. Because the data are very limited for analysis, so we can only conclude that with more practice, people will earn this procedure. Based on that people can learn from practice, we can let an authenticated user practice a lot for a specific angle, thus he or she can perform the movement pretty accurate and skillfully. But other unauthenticated users do not know how is the mouse modified and how would the authenticated user perform. Therefore, others cannot be recognized as authenticated user. Our experiment can be used as a user authentication method not only on mouse of computer, but also touchpads and touchscreens.

## 6.2 Future Work

Also, there is much future work for our research. The limitation and disadvantage of our research is that the data collected and the number of subjects is very small. Without big data, we can't find the accurate learning process stereotype for each subjects and we cannot find the exact level of subjects of their learning process.

Besides, in this experiment there is no incentive for subjects. From the limited experiments we conclude that lack of incentive will severely influence the learning process of subjects.

Practicing and learning can cause fatigue and loss of patience, which actually influenced the behavior of subjects. Lack of incentive even cause some subjects giving up learning, making data collected meaningless. In the future work we will provide incentives to subjects to make sure the quality of data collection.

There is possibility that based on lot of subjects and huge amount of data we can work on machine learning algorithm that can find the stereotype and features of every subject. Although our objective is to implement our approach in the scenarios with single user, we can still try to improve the work so possibly it can be used in the multi-user scenarios. With the stereotype and features calculated by certain machine learning algorithm we can build the database that stores the special features of people. This approach will be very challenging but also very interesting. To find the stereotype in mouse movement of a person will be very useful not only in the mouse dynamics based user authentication field. Finding the stereotype of certain dynamics and biometrics can also be used in other biometrics based people recognition or authentication, such as speech and keyboard stroke. This direction is very promising, interesting and is worth for searching and exploring.

# REFERENCES

[1] S M Bellovin and M Merritt. Limitations of the kerberos authentication system. submitted to Computer Communication Review 5, June 1990.

[2] Glaus Vielhauer. *Biometric User Authetication for IT Security: From Fundamentals to Handwriting*. 2005.

[3] A. Kumar and K. V. Prathyusha. Personal authentication using hand vein triangulation and knuckle shape. *IEEE Trans. Image Processing*, 18(9):2127–2136, 2009.

[4] R. Janakiraman and T. Sim. Keystroke dynamics in a general setting. In *Biometric Authentication*, pages 584–593, 2007.

[5] Rick Joyce and Gopal K. Gupta. Identity authentication based on keystroke latencies. *Commun. ACM*, 33(2):168–176, 1990.

[6] Saleh Ali Bleha and Mohammad S. Obaidat. Dimensionality reduction and feature extraction applications in identifying computer users. *IEEE Transactions on Systems, Man, and Cybernetics*, 21(2):452–456, 1991.

[7] Daw-Tung Lin. Computer access authentication with neural network based keystroke identity verification. In *IEEE International Conference on Neural Networks (IJCNN'97)*, volume I, pages I–174–I–178, Houston, TX, June 1997. IEEE. Chung-Hua Ploytechnic Institute, .tw.

[8] Saleh Bleha, Charles Slivinsky, and Bassam Hussein. Computer-access security systems using keystroke dynamics. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, PAMI-12(12):1217–1222, December 1990.

[9] J. A. Robinson, V. W. Liang, J. A. M. Chambers, and Christine L. MacKenzie. Computer user verification using login string keystroke dynamics. *IEEE Transactions on Systems, Man, and Cybernetics, Part A*, 28(2):236–241, 1998.

[10] Mohammad S. Obaidat and Balqies Sadoun. Verification of computer users using keystroke dynamics. *IEEE Transactions on Systems, Man, and Cybernetics, Part B*, 27(2):261–269, 1997.

[11] Lívia C. F. Araújo, Luiz H. R. Sucupira, Miguel Gustavo Lizárraga, Lee Luan Ling, and João Baptista T. Yabu-uti. A fuzzy logic approach in typing biometrics user authentication. In *Proceedings of the 1st Indian International Conference on Artificial Intelligence, IICAI 2003, Hyderabad, India, December 18-20, 2003*, pages 1038–1051. IICAI, 2003.

[12] Willem G. de Ru and Jan H. P. Eloff. Enhanced password authentication through fuzzy logic. *IEEE Expert*, 12(6):38–45, 1997.

[13] Y. S. Shin. Biometric identification system based on dental features. In *Biometric Authentication*, page 229, 2005.

[14] Jiankun Hu, Don Gingrich, and Andy Sentosa. A k-nearest neighbor approach for user authentication through biometric keystroke dynamics. In *ICC*, pages 1556–1560. IEEE, 2008.

[15] Fabian Monrose, Michael K. Reiter, and Susanne Wetzel. Password hardening based on keystroke dynamics. *Int. J. Inf. Sec*, 1(2):69–83, 2002.

[16] Jiankun Hu, Don Gingrich, and Andy Sentosa. A k-nearest neighbor approach for user authentication through biometric keystroke dynamics. In *ICC*, pages 1556–1560. IEEE, 2008.

[17] L. C. F. Araujo, L. H. R. Sucupira, M. G. Lizarraga, L. L. Ling, and J. B. T. Yabu Uti. User authentication through typing biometrics features. In *Biometric Authentication*, pages 694–700, 2004.

[18] Finger vein authentication device. In Stan Z. Li and Anil K. Jain, editors, *Encyclopedia of Biometrics*, page 424. Springer US, 2009.

[19] Ahmed Awad E. Ahmed and Issa Traoré. A new biometric technology based on mouse dynamics. *IEEE Trans. Dependable Sec. Comput*, 4(3):165–179, 2007.

[20] S. Hocquet, J. Y. Ramel, and H. Cardot. User classification for keystroke dynamics authentication. In *Biometric Authentication*, pages 531–539, 2007.

[21] Francesco Bergadano, Daniele Gunetti, and Claudia Picardi. User authentication through keystroke dynamics. *ACM Trans. Inf. Syst. Secur*, 5(4):367–397, 2002.

[22] Eric Flior and Kazimierz Kowalski. Continuous biometric user authentication in online examinations. In Shahram Latifi, editor, *Seventh International Conference on Information Technology: New Generations, ITNG 2010, Las Vegas, Nevada, USA, 12-14 April 2010*, pages 488–492. IEEE Computer Society, 2010.

[23] A. Humm, J. Hennebert, and R. Ingold. Combined handwriting and speech modalities for user authentication. *IEEE Trans. Systems, Man and Cybernetics*, 39(1):25–35, January 2009.

[24] Maja Pusara and Carla E. Brodley. User re-authentication via mouse movements. In Carla E. Brodley, Philip Chan, Richard Lippmann, and William Yurcik, editors, *Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC 2004), 29 October 2004, Washington DC, USA*, pages 1–8. ACM, 2004.

[25] Chao Shen, Zhongmin Cai, Xiaohong Guan, Youtian Du, and Roy A. Maxion. User authentication through mouse dynamics. *IEEE Transactions on Information Forensics and Security*, 8(1):16–30, 2013.

[26] Bassam Sayed, Issa Traoré, Isaac Woungang, and Mohammad S. Obaidat. Biometric authentication using mouse gesture dynamics. *IEEE Systems Journal*, 7(2):262–274, 2013.

[27] Farnaz Towhidi and Maslin Masrom. A survey on recognition based graphical user authentication algorithms. *CoRR*, abs/0912.0942, 2009.

[28] Romain Giot, Mohamad El-Abed, Baptiste Hemery, and Christophe Rosenberger. Unconstrained keystroke dynamics authentication with shared secret. 2011.

[29] John W Krakauer and Reza Shadmehr. Consolidation of motor memory. *Trends in neurosciences*, 29(1):58–64, Jan 2006.

[30] https://en.wikipedia.org/wiki/Linux.

[31] Jonathan Corbet, Alessandro Rubini, and Greg Kroah-Hartman. *Linux device driver, 3ed.* 2005.

[32] https://en.wikipedia.org/wiki/Qt.