Security using Fusion of Keystroke and Mouse Dynamics (Result Paper)

Authors
Yogesh R.Nagargoje¹, Dr.Santosh S.Lomte², Prof.Rajesh.A.Auti³, Anil H.Rokade⁴

Email-yogeshspwec@gmail.com, santoshlomte@hotmail.com, rajeshauti24@gmail.com
mr.anil2097@rediffmail.com

Student, Department of Computer, Dr. SeemaQuadri Institute of Tech, Aurangabad, India¹
Professor, Department of Computer, Dr. SeemaQuadri Institute of Tech, Aurangabad, India²
Asst.Professor, Department of Computer, Dr. SeemaQuadri Institute of Tech, Aurangabad, India³
Student, Department of Computer, Dr. SeemaQuadri Institute of Tech, Aurangabad, India⁴

ABSTRACT

In today's world, username and password is the most common way to authenticate the person. Stolen username and passwords can be helpful in order to commit suspicious hacking activity. Keystroke biometric authentication provides additional user characteristics which includes typing style to authenticate the user. Pointing device such as touchpad's and mice are getting more importance due to cheap cost and easy availability in behaviour-based user authentication. Mouse Dynamics focuses on the problem of authentication by verifying the user based on single or double clicks. Features are extracted from the mouse dynamics to find out the uniqueness of the user.

We introduce the mixing of keystroke and mouse dynamics to authenticate the user based on the keystroke and mouse movements. Keystroke dynamics authenticate the user by capturing password. The features are extracted and threshold is set to give an access to the system. Mouse dynamics provides the fixed mouse related task such as single click or double clicks. The unique mouse features and template is generated. The results from the keystroke and mouse dynamics are gathered, and outcome shows the results.

Keywords- Keystroke dynamics, Network Security, Mouse Dynamics, Security issues and Password hardening.

INTRODUCTION

Keystroke analysis is the user’s identity through their way of typing on a computer keyboard. Typed key measurements are available from most every keyboard can be recorded to determine ‘Dwell time’ (The time a key pressed) and ‘Flight time’ (The time between “key down” and the next “key down”). The recorded
Keystroke timing data is processed through an algorithm, which determines a primary pattern for the future comparisons. The only required hardware is the standard keyboard that comes with every computer. The system does not require sensors or other additional hardware. Keystroke analysis can completely replace password procedure on the Internet. Users do not have to remember a password. It is highly secure because keystroke behaviour cannot be imitated, stolen, forgotten or misplaced. The system will not be fooled by the typing rhythms of a language different from the one of the user’s profiles used by the intruder.

**BIOMETRIC TECHNOLOGY**

A BIOMETRIC SYSTEM PROVIDES AUTOMATIC RECOGNITION OF AN INDIVIDUAL BASED ON SOME SORT OF UNIQUE FEATURE OR CHARACTERISTIC POSSESSED BY THE INDIVIDUAL. BIOMETRIC SYSTEMS HAVE BEEN DEVELOPED BASED ON FINGERPRINTS, FACIAL FEATURES, VOICE, HAND GEOMETRY, HANDWRITING, THE RETINA, AND THE ONE PRESENTED IN THAT THESIS, THE IRIS. MOST BIOMETRIC SYSTEMS ALLOW TWO MODES OF OPERATION. AN ENROLMENT MODE FOR ADDING TEMPLATES TO A DATABASE, AND AN IDENTIFICATION MODE, WHERE A TEMPLATE IS CREATED FOR AN INDIVIDUAL AND THEN A MATCH IS SEARCHED FOR IN THE DATABASE OF PRE-ENROLLED TEMPLATES.

**KEYSTROKE BIOMETRICS:**

Today the username and password is the regularly used authentication method. Computers store the vast amount data which is private and sensitive data. The level of perfection is not up to the mark. This authentication method can be compromised with the security of the user. It’s important to increase the level of confidentiality.

Improvising password method, interaction of the user with the computer utilizes as a parameter to the security. The most promising technique where user’s typing style considers as an authentication method called as Keystroke biometrics.

Features related to Keystroke Dynamics:

1. **Dwell time**
   It’s the time between Key press and key release.

2. **Flight time**
   It’s the time between Key press and key press, key release and key release[4].

The combining of keystroke authentication with the password based system adds a layer of security which takes care of the shortcomings of the passwords. The legitimate user’s password as well as the typing style in terms of the timing (dwell time and flight time) are input to the system which makes hard to crack the password as well as the keystroke timings. This promising technique is yet to be accepted by the users.
The username password system still presents. We added the keystroke parameter which is to be entered by the user and the keystroke parameters are extracted and template is generated. The parameters include keystroke dwell time, flight time.

To experiment the method, a group of people performed the task of entering the username, password. The process separates into the two parts. First the username-password matching is done by the system, and then keystroke parameters are extracted from the passphrase. The matching of keystroke parameters is done in the second part. The mixing of the results is shown to the user as a single result and the user is either accepted or rejected.

**FIGURE 1.1 KEystroke DYNAMICS**

**MOUSE DYNAMICS:**

In today’s world, the security of delicate system is still an issue. Many applications use the mobile based authentication by providing the random number on the registered mobile. These kinds of systems need an additional level of security. Behavioural biometrics helps to improvise the security of such delicate systems. Mouse dynamics is a part of behavioural biometrics which can authenticate the user with the less amount cost. The handling of mouse is a parameter to the security in mouse dynamics.

**FIGURE 1.2 MOUSE DYNAMICS**

**FEATURES RELATED TO MOUSE DYNAMICS:**

**SINGLE CLICK TIMINGS**

It’s the time duration between two single clicks of mouse.

**DOUBLE CLICK TIMINGS**

It’s the time duration between two double clicks of mouse.
1.5 Necessity

Keystroke Biometrics

Today the username and password is the regularly used authentication method. Computers store the vast amount data which is private and sensitive data. The level of perfection is not up to the mark. This authentication method can be compromised with the security of the user. It’s important to increase the level of confidentiality.

Improvising password method, interaction of the user with the computer utilizes as a parameter to the security. The most promising technique where user’s typing style considers as an authentication method called as Keystroke biometrics.

The combining of keystroke authentication with the password based system adds a layer of security which takes care of the shortcomings of the passwords. The legitimate user’s password as well as the typing style in terms of the timing (dwell time and flight time) are input to the system which makes hard to crack the password as well as the keystroke timings. This promising technique is yet to be accepted by the users.

1.6 Objective

To evolve a method for user authentication
To establish user authentication with minimum hardware
To provide high level of security to the users
To achieve the authentication with minimal cost
To carry performance analysis of suggested architecture.

fingerprints are more likely to be homosexually oriented, etc.

RELATED WORK

Most of the papers used statistical methods and neural networks for keystroke based authentication. [3] proposed a Monte Carlo approach for data collection and parallel decision tree (DT) for identifying the genuine user. Data collection included six basic parameters by comparing key press and key release of successive keys. A vector formed on the basis of raw data. Wavelet analysis was performed on four 16-element sub vectors by splitting the keystroke feature vectors and eight DT classifiers were trained for every user. Almost 19 times training data generated at the training level and eight decision trees were formed on the basis of raw data. User gets an entry to the system if and only if user matches any of the three decision trees. The average FRR (False rejection rate) was 9.62% and FAR (false acceptance rate) was 0.88%.

Complexity of the algorithm depends upon the number of characters in the string. Adding a new user without disturbing the entire system was tedious task.

Author suggested that keystroke mechanism can be used to identify the imposter when he gets hold of the secret PIN and password. [4] In this paper two algorithms were proposed to implement the keystroke efficiently. The resulted mean, standard deviation and weight formula used to calculate the weight in first
step. In second step, the login time keystroke data is compared with the registered mean± standard deviation which resulted into match count. If both conditions are satisfied with 50% and 75% respectively then, user successfully logs on the system. This paper produced FRR which was almost zero and FAR ranged between 0.12% and 0.28%.

Author suggested a different technique to strengthen the password system by combining with keystroke biometrics. [5] In this paper author proposed fusion of two algorithms named as Gaussian probability density function and direction similarity measure. The fusion of two algorithms is done by different methods and among them AND rule showed the best result. This paper showed FRR and FAR as 1%. Calculated EER reported as 1.401% which helps the security concern. Retraining process is also discussed in this paper which helps in updating the template.

**Research in Keystroke:**

Researchers are interested in using this keystroke dynamic information, which is normally discarded, to verify or even try to determine the identity of the person who is producing those keystrokes. This is often possible because some characteristics of keystroke production are as individual as handwriting or a signature. The techniques used to do this vary widely in power and sophistication, and range from statistical techniques to neural-network to artificial intelligence.

**Keystroke Biometrics**

Today the username and password is the regularly used authentication method. Computers store the vast amount data which is private and sensitive data. The level of perfection is not up to the mark. This authentication method can be compromised with the security of the user. It’s important to increase the level of confidentiality.

Improvising password method, interaction of the user with the computer utilizes as a parameter to the security. The most promising technique where user’s typing style considers as an authentication method called as Keystroke biometrics.

The combining of keystroke authentication with the password based system adds a layer of security which takes care of the shortcomings of the passwords. The legitimate user’s password as well as the typing style in terms of the timing (dwell time and flight time) are input to the system which makes hard to crack the password as well as the keystroke timings. This promising technique is yet to be accepted by the users.

**IMPLEMENTATION**

The keystroke and mouse system is part of advanced security level of security. The username-password system shows a low level security for the hacker. We have implemented the system by extracting the parameters from the keystroke and mouse. The dwell and flight time parameters are extracted from the keystroke and the combination of dwell and flight time shows the higher accuracy than the individual one.
To improve the results we have checked the mouse dynamics. The use of single clicks and double clicks are also added. The double clicks show the improved results than the single click.

We have provided username password system to the user. Every user has to enter the username and password into the system. As the user enters the password, the keystroke parameters are calculated using dwell and flight time. The key press and key release show the values in milliseconds. The mouse dynamics is provided with the task. The mouse dynamics shows the single and double clicks statistics. The mouse double clicks show better results.

We have used SVM (support vector machines). SVM is generally used for image processing. The use of algorithm is done for the separation of imposter and genuine user. The SVM takes care of the user’s security and provides the best outcome. We have tested the system for 16 users using keystroke and mouse.

RESULTS AND ANALYSIS

We have done experimentation of users for the results and analysis. The Following parameters come in to the picture.

Dwell Time Results:

Figure 3 shows the dwell time results. X-axis shows the users and Y-axis shows the accuracy in percentages. The two lines show FAR and FRR results. The results show 24% EER where FAR and FRR meets. The promising results show that the use of dwell time is not the solution of keystroke system.

![Dwell Time](image)

**Figure 4.1** Dwell time results

Flight Time Results:
Figure 4 shows the Flight time results. X-axis shows the users and Y-axis shows the accuracy in percentages. The two lines show FAR and FRR results. The results show 20% EER where FAR and FRR meet. The promising results show that the use of Flight time is not the only solution of keystroke system.

![Flight time graph](image)

**Figure 4.2** Dwell time results

**Dwell And Flight Time**

Figure 5 shows the Dwell and Flight time results. X-axis shows the users and Y-axis shows the accuracy in percentages. The two lines show FAR and FRR results. The results show 5% EER where FAR and FRR meet. The promising results show that the use of Dwell and Flight time is the only solution of keystroke system.

![Dwell and Flight time graph](image)

**Figure 4.3** Dwell and flight time results

**Single Click Timings**

Figure 6 shows the single click results. X-axis shows the users and Y-axis shows the accuracy in percentages. The two lines show FAR and FRR results. The results show 22% EER where FAR and FRR meet. The promising results show that the use of single click time is not only solution of mouse system.
Double Click Timing

Figure 7 shows the single click results. X-axis shows the users and Y-axis shows the accuracy in percentages. The two lines show FAR and FRR results. The results show 6% EER where FAR and FRR meets. The promising results show that the use of double click time is only solution of mouse system.

Dwell, flight and Single click Timings
Figure 4.6 Keystroke and mouse results

Figure 8 shows the Keystroke and mouse results. X-axis shows the users and Y-axis shows the accuracy in percentages. The two lines show FAR and FRR results. The results show 2% EER where FAR and FRR meet. The promising results show that the use of double click time and combination of dwell and flight time is solution of security.

CONCLUSIONS

The keystroke and mouse features are combined and provides a high level security using keystroke parameters called as dwell and flight time. These keystroke parameters are combined with the mouse parameters to provide high level of security. The combination of dwell and flight time with single click shows better results. The accuracy of combination of keystroke and mouse authentication shows more than 80%. The future scope includes the identification of other parameters and the use of another algorithm to improvise the level of security. Multimodal biometrics can be easily used to find out the good results using keystroke biometrics.

ACKNOWLEDGEMENT

It is my great pleasure in expressing sincere and deep gratitude towards my guide Dr. Santosh S. Lomte. I am also thankful to Head of Department of Computer Science and Engineering, Prof. Rajesh. A. Auti for providing me various resources and infrastructure facilities.

I also offer my most sincere thanks to Principal Prof. Venkatesh Gaddime, Everest College of Engineering, Aurangabad, my colleagues and staff members of computer science and Engineering department, Everest college of Engineering, Aurangabad for cooperation provided by them in many ways.
REFERENCES


   A. Peacock: Learning User Keystroke Latency Patterns (Preliminary Report),


