DEVELOPING A TIGHTER AUTHENTICATION SECURITY MECHANISM USING KEYSTROKE DYNAMICS

BY

Duches Dianne B. Castañeda

Khimy Jyanina L. Iñigo

Larence O. Lao

SCHOOL OF ARTS AND SCIENCES

ATENEO DE DAVAO UNIVERSITY

MARCH 2005

DEVELOPING A TIGHTER AUTHENTICATION SECURITY MECHANISM USING KEYSTROKE DYNAMICS

An Independent Research

Presented to

The Faculty of the Computer Studies Division

Ateneo de Davao University

In Partial Fulfillment

of the Requirements for the Degree

Bachelor of Science major in Computer Science

by

Duches Dianne B. Castañeda

Khimy Jyanina L. Iñigo

Larence O. Lao

SCHOOL OF ARTS AND SCIENCES

ATENEO DE DAVAO UNIVERSITY

MARCH 2005

TABLE OF CONTENTS

DEVELOPING A TIGHTER AUTHENTICATION SECURITY MECHANISM USING KEYSTROKE DYNAMICS

By

Duches Dianne B. Castañeda
Khimy Jyanina L. Iñigo
Larence O. Lao

Abstract:

As technology advances, information management systems become more powerful and information security enforcement becomes more critical. This paper presents a more secure approach in authenticating users. It uses keystroke dynamics by employing a combination of the conventional approach and of the neural networks. This combined approach not only deals with users' conventional textual passwords but also with its corresponding unique typing patterns for tighter and more secure authentication. To achieve this, the proponents planned to have five phases in implementing keystroke dynamics: the Initialization stage, the Data Collection stage, the Retrieval Phase, the Adaptability stage, and the Recovery phase.

Keywords:
Security, biometrics, keystroke dynamics, neural networks

CHAPTER 1

INTRODUCTION

As technology advances and information management systems become more powerful, the problem of enforcing information security also becomes more critical. Current security mechanisms cannot cope up with the technological revolution (e.g. the increase of online and offline identity theft and malicious attacks). In addition, people can easily avail software applications that can hack and/or crack user passwords. Having this knowledge, offenders can harm the system as well as the user. Thus, there is a need for tighter security mechanisms.

1.1 Background of the Study

With the increase of identity theft through hacking and cracking, the system must have a way to authenticate user identification. An effective way to validate one's identity is using biometrics. Biometrics is the statistical analysis of biological observations, which consists of physical and behavioral attributes. Physical biometrics defines biological aspects of a person, such as DNA, fingerprint, iris, retina, hand geometry, and vein structure, which determine identity. On the other hand, behavioral biometrics defines characteristic traits of a person, such as handwriting, speech, language removal, gait, gesture, and typing patterns, which determine identity.

Many believe that physical biometrics is more effective than behavioral biometrics. However, studies show that behavioral biometrics outweigh most physical biometrics. The studies have the following criteria: operation, technical, financial, manufacturing, and connectivity. Results are as follows:

- The finger print method is very accurate although associated with criminality by some people. It needs and uses a finger print scanner.
- The iris recognition method is very accurate, but has acceptance problems. In order to recognize the person's identity, it uses a retinal scanner.
- The facial analysis method works well but is sensitive to facial angles and lighting. It needs a camera to capture the person's face and uses a software application that checks for the identity.
- The hand geometry method is accurate and well accepted, but expensive. It uses a special hand scanner device.
- The hand written signature verification is also highly acceptable but not as accurate. It needs a special device that recognizes a person's signature.
- Speech analysis is mostly appropriate for voice-based systems. It requires a speech recognition device.

Among the biometrics, studies concluded that keystroke dynamics has the potential of being the most appropriate for the users' needs. This method is simple, cheap, convenient and transparent to the user. Moreover, keyboards are also commonly available.

Many companies have tried to commercialize such technique. Unfortunately, all of them were unsuccessful in securing information because of three main reasons: inaccurate production of hardened password, login delay, and lack of standardization among keyboards. This challenges the proponents to strengthen the keystroke dynamics approach by having a more accurate production of the typing patterns and minimizing the login delay.

1.2 Statement of the Problem

This study sought to answer the general problem: How can a tighter authentication security mechanism at both the clients and the servers of a network be implemented using keystroke dynamics?

Specifically, this study sought to answer the following problems:

- How can keystroke dynamics tighten security and ensure authentication?
- What are the different approaches in implementing keystroke dynamics?
- What is the most effective approach in tightening security using keystroke dynamics?
- What are the ways to minimize login delays in keystroke dynamics implementation?
- What are the ways to lessen time variability in the initialization phase of a keystroke dynamics implementation?
- What are the factors affecting keystroke dynamics?

- What makes this study more effective than the current keystroke dynamics technologies?

1.3 Objectives of the Study

This study aimed to develop a tighter authentication security mechanism at both the clients and the servers of a network using keystroke dynamics.

Specifically, this study aimed to:

- Determine how keystroke dynamics tighten security and ensure authentication
- Name the different approaches in implementing keystroke dynamics
- Identify the most effective approach in tightening security using keystroke dynamics
- Enumerate the ways to minimize login delays in keystroke dynamics implementation
- List the ways to lessen time variability in the initialization phase of a keystroke dynamics approach
- Name the factors affecting keystroke dynamics
- Specify the features that make this study more effective than the current keystroke dynamics technologies

1.4 Scope and Limitation of the Study

Since the usage of textual passwords is the principal authenticating security technique, the study generally focuses on keystroke dynamics. The proponents wanted to address the current problems in keystroke dynamics such as security, adaptability, and accuracy issues.

The project team tried to implement a prototype of an enhanced BioPassword. They implemented a system that lessens the variable time in the initialization phase, that has a recovery phase, and that is lenient enough and strict enough to adapt to the user's typing pattern changes. Both client and server users in a network can benefit from this improved system.

The proponents used C# of Visual Studio .NET. They evaluated the results of this study by comparing the false acceptance rate (FAR) and false rejection rate (FRR) with the rates from current keystroke dynamics technologies.

This study did not intend to address the issue on keyboard standardization. Moreover, the projected prototype is limited to run only in Windows 2000 and higher Windows platforms.

1.5 Significance of the Study

This study is significant for both client and server users. Through knowing the user's typing pattern with the use of keystroke dynamics, end-users and server administrators will be able to have tighter security, preventing malicious attackers in obtaining important information about the company and its users.

1.6 Definition of Key Terms

1. Biometrics – is a unique, measurable characteristic or trait of a human being that verifies one's identity.
2. Keystroke dynamics – is a method of making computer passwords harder to crack by recording not only the user's password but also the way that the user types it.
3. Identification – is when the system collects a larger amount of keystroke dynamics, which helps in identifying the user on previously collected information of keystroke dynamics profiles of all users.
4. Verification – is when the system identifies the identity of the user, usually at login time, by measuring the typing pattern when writing the username and the password and comparing measurements to a previously stored profile.
5. Neural networks – is a mathematical model for information processing based on a connectionist approach to computation.
6. Adaptive learning – is the ability of neural networks to learn how to do task based on the data given for training or initial experience.
7. Self-organization – is the ability of neural networks to create its own organization or representation of the information it receives during learning time.
8. Flight time – is the amount of time it takes a person to between keys.
9. Dwell time – is the amount of time one holds down a particular key.
10. Key digraph – is a set of two adjacent keystrokes.

11. Outliers – is an observation that lies an abnormal distance from other values in a random sample from a population.
12. Variance – used to characterize the variability of the distribution (e.g. user's keystroke pattern).
13. Pooled variance – is a single estimate of the common variance obtained by combining the estimated variances from each of several samples.
14. False Acceptance Rate (FAR) – is the rate of acceptance of invalid users.
15. False Rejection Rate (FRR) – is the rate of rejections of valid users.
16. Failure-to-Enroll Rate (FER) – is the ability of the biometric to enroll a biometric for a user.
17. Equal Error Rate (ERR) – is the crossover point when FRR is equal to FAR.