



**AN APPROACH
TOWARDS PASSWORD PROTECTION
BASED ON TYPING STYLE**

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

NELUM CHATHURANGA AMARASENA

December 2014

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Mr. Yasas Mallawarachchi (Supervisor)

Approved for M.Sc. Research Project:

Mr. Prasanna S. Heddala
M.Sc. Research Project Coordinator, SLIIT

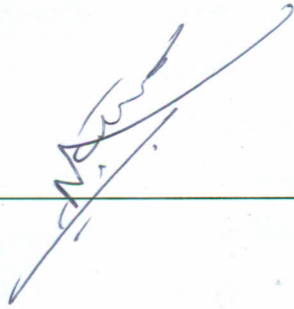
Approved for M. Sc.:

Coordinator, SLIIT M.Sc. Program

Declaration of Originality

"I certify that this dissertation does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any University: and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where due reference is made in the text."

Signed _____

A handwritten signature in blue ink, appearing to be 'M. J. ...', written over a horizontal line.

Date _____

19/01/2015

Acknowledgements

At Sri Lanka Institute of Information Technology, I have benefited of having a great panel of lecturers, supervisors and all the other staff who were always there for support, advice and instructions to be given. Mr. Yasas Mallawarachchi was a really supporting, encouraging and motivating supervisor, providing; advice, constant constructive criticism of my ideas and writing, also spending his time for guiding me throughout my study, and the freedom to work on my own ideas and concepts. Therefore my heartiest thank to my research supervisor Mr. Yasas Mallawarachchi.

This project could not have been completed without the supports I received from many individuals by participating in my research and also in many other ways at different stages of the research. I would like to thank all my lecturers who made me the person to conduct a research with all knowledge and skills. I express my thanks to my mother and father who always encouraging me to accomplish this research since I missed it in the last year.

My special thank to my wife, Mrs. Thilanka Dhananjanie for providing her constant support and ideas to complete the study with better standards because that support was really energetic. Thanks to all my friends who were supported me in different aspects in this context and those who motivated me to complete the research during this year. My special thank goes to Mr. Lasantha for the priceless help provided in my literature findings by giving me an opportunity to browse through IEEE publications related to the keystroke dynamics.

I would like to thank all the researchers for their research work, findings and publications in the area of keystroke dynamics because if they did not overlook this challenging area of biometric I may not have ever persuaded.

Finally, but not least, I would like to express my gratitude to my institution and friends; without whose support this project would be a distant reality. Thanks for everything that helped me get to this success.

Table of Contents

Contents

Declaration of Originality.....	ii
Abstract.....	iii
An Approach towards Password Protection Based On Typing Style.....	iii
Acknowledgements.....	iv
Table of Contents.....	v
List of Figures.....	viii
1 INTRODUCTION.....	1
1.1: Study Background.....	1
1.1.1: What is a Password?.....	1
1.1.2: Usage of Passwords.....	1
1.1.3: Magnitude of Defending Passwords.....	2
1.1.4: Keystroke Dynamics.....	3
1.2: Aim and Objectives.....	4
1.2.1: Aim.....	4
1.2.2: Objectives.....	5
2 LITERATURE REVIEW.....	7
2.1: Introduction.....	7
2.2: Password Protecting Mechanisms.....	7
2.2.1: Avoiding Key Loggers.....	8
2.2.2: Graphical User Authentication.....	9
2.2.3: Authentication without Identities.....	9
2.2.4: Authentication in Social Network.....	9
2.2.5: One Time Password.....	10
2.2.6: Virtual Password Mechanism.....	10
2.3: Biometric Authentication.....	11
2.4: Key Stroke Dynamics.....	13
2.4.1: Overview.....	13
2.4.2: Development Platform.....	15

3	DATA & METHODOLOGY	18
3.1:	Introduction (not what you type, but how you type)	18
3.2:	Data	18
3.2.1:	Data Acquisition.....	18
3.2.2:	Data Size	19
3.2.3:	Data Type	19
3.2.4:	Genuine and Imposter Samples.....	20
3.2.5:	Input Repetition.....	20
3.2.6:	Public Data Set	21
3.3:	Methodology	21
3.3.1:	Scheme of Keystroke Dynamics	21
3.3.2:	Feature Selection and Usage	24
3.3.3:	Di-Graph	25
3.3.4:	N-Graph.....	28
3.3.5:	Classification.....	28
3.3.6:	Retraining Module	32
3.3.7:	Outlier Handling.....	34
3.3.8:	Fusion and Multimodal	35
3.3.9:	Keystroke Dynamics Quality Measure and Control	37
4	RESULTS & DISCUSSION	40
4.1:	Introduction.....	40
4.2:	Results.....	40
4.2.1:	The Password Hardening Toolkit (Toolkit)	40
4.2.2:	Usage of the Toolkit.....	42
4.2.3:	A Sample Results	43
4.3:	Length of the String	50
4.4:	Appreciation & Confidence	50
5	CONCLUSION	52
5.1:	Introduction.....	52
5.2:	Password Hardening	52
5.3:	Security in Multifactor Authentication Systems.....	53

5.4: Limitations53

5.4.1: Storing the Pattern54

5.5: Future Work54

5.5.1: Modeling Keyboard55

5.5.2: Non-English Sequences55

5.5.3: Key Stroke Pressure56

Bibliography57

List of Figures

Figure 2.1: Overview of different biometric authentication approaches.....	12
Figure 2.2: Graph clearly indicates an increasing trend on research work.....	14
Figure 2.3: A general timeline on the overview of keystroke research work evolution.....	15
Figure 3.1: The percentage distribution of various types of input data.....	19
Figure 3.2: General synopsis of a common biometric system.....	22
Figure 3.3: The percentage distribution of feature data extracted for keystroke experiment in the literature.....	25
Figure 3.4: Figure depicts the different keystroke events of two characters “j” and “Y” alongside with the formation of dwell time and flight time	26
Figure 3.5: Percentage distribution among classification methods employed by keystroke research work	30
Figure 4.1: A screen shot of the “Password Hardening Toolkit”	41
Figure 4.2: Recording password (Step 1)	43
Figure 4.3: Training round 1 (Step 2).....	44
Figure 4.4: After training round 3 (Step 2).....	47
Figure 4.5: Completion of the Training Phase (Step 2).....	48
Figure 4.6: Unsuccessful try, text OK, but pattern is not (Step 3)	49
Figure 4.7: Successful try, text and the pattern both OK (Step 3).....	49
Figure 4.8: General appreciation of keystroke dynamic system	51
Figure 4.9: Users’ confidence about the keystroke dynamic system.....	51

Abstract

An Approach towards Password Protection Based On Typing Style

Nelum Chathuranga Amarasena

M. Sc. in Information Technology

Supervisor: Mr. Yasas Mallawarachchi

December 2014

The most common user authentication mechanism is password verification. In other words, characters which types as text in a password field. However, the aim of this research is to find out whether the rhythm and/or the style of typing; how types instead of what types (Keystroke Dynamics), is sufficiently reliable as a security enhancement. This is a biometric approach. Biometric solutions are costly; requires at least one additional sensor. But this study focuses on an economical biometric solution that does not necessitate any additional sensor other than the keyboard. Keystroke dynamics is an interesting biometric because it always invisible for users, unless they are physically present, and also it is not depending on a dedicated device or hardware infrastructure. When a person is typing at a keyboard, the detailed timing information that describes exactly when each key was pressed and when it was released and variation of speed moving between two keys are continuously monitoring in order to recognizes a unique pattern. Then another pattern recognition part is operating in stealth mode with the password verification. Therefore after the password is verified successfully, the pattern recognition part also needs to be completed in order to authenticate the user. Significance of this research is the way of generating and storing the pattern. As I explained through the literature study keystroke dynamics is not a very reliable biometric. So the challenge was to make a strong pattern which is hard to reveal using a less reliable building block which I achieved successfully through this study.