A Comparison between Human Selected, Derived and System-Generated Passwords in terms of Keystroke Dynamics

N Pavaday*
Faculty of Engineering,
University of Mauritius, Reduit
n.pavaday@uom.ac.mu

K M S Soyjaudah
Department of Electrical and Electronics Engineering
Faculty of Engineering
University of Mauritius, Reduit
ssoyjaudah@uom.ac.mu

Abstract

Pure hardware based biometric systems of user authentication have low rate of errors but increase computational and economic cost. Alternate biometric methods based purely on software development are now booming. This paper presents our results on improving authentication of users using a password mechanism hardened with keystroke timing vectors. We develop a system that is trained with the keystroke timing vectors of the owners and then later used to differentiate between authentic users and impostors. Using a prototype implementation of our scheme, we compare the results of human-selected, derived passwords and system generated to reveal the practical viability of our approach in terms of results achieved, ease of implementation and use.

Keywords: Security, Biometric, Behavioral, Keystroke dynamics, Password

* To whom correspondence should be addressed

1. INTRODUCTION

Computerized systems reside at the heart of a number of systems, on which people rely heavily. Unfortunately many of these systems are vulnerable to attack, misuse, and abuse that can inhibit their operation, corrupt valuable data or expose private information. Computer security usually involves a number of components among which successful verification of the identity of a person/entity willing to use the system stands as the essential front line of defense (Pfleeger C.P, 1997). Effective system administration, auditing, and efficient resource management all hinge on accurate user identification (Jobusch D.L & Oldehoeft A.E,1989); (Pfleeger C.P,1993); (Spender J.C,1987). Authentication requires users to prove that they really are who they say they are; before being given authorization which then dictates what the users can access (Roland,2004). Biometric mechanisms are now considered as the strongest way to authenticate people (Bolle R, 2003), (Hsu R et al, 2002).

As human beings, we have characteristics that differentiate us from others. Our genetic code, fingerprints, handwriting and ocular retinal pattern are all examples of biometric features that make us unique and distinguishable as individuals. The typing pattern of a person, when using a keyboard (Joyce R & Gupta G, 1990), (Mandujano S & Soto R, 2004); falls into the behavioral biometric category and has the advantage of not requiring any costly equipment.
This paper is structured as follows. We begin by discussing the authentication problems as well as those associated with the de facto password based mechanism and the motivation for a biometric solution based on typing rhythms to enhance the former. Section 2 introduces the concept of authentication while section 3 reviews previous work in that field using keystroke dynamics as well as some implementation types. In the subsequent section we describe our technical solution applied in the study. Section 4 details the experimental results obtained using two variants of the prototype. After that, we present results of our preliminary experiment with a reduced sample of the population. Finally, we provide some conclusions and possible extensions to the method.

2. AUTHENTICATION

The triangle of authentication consists mainly of (i) Possession of object; e.g. locks, keys, smart cards and magnetic-strip cards. (ii) Knowledge of specific information or answers to questions. The de facto standard use for stand alone and remote authentication falls under this category (Jobusch D.L. & Oldehoeft A.E, 1989) (iii) The third type, what the person is, requires the authentication device to measure a characteristic of the person being verified (Ru W.G and Eloff J.H.P, 1993). The latter, biometric, can be sub divided into two categories: those that use physical characteristics, such as fingerprints, face, retina scans, iris and hand geometry and those that use behavioral characteristics, such as signature, voice and keystroke dynamics.
Each authentication scheme category has its strengths and weaknesses. Possession based authentication is susceptible to loss or theft and in some cases copying/cloning as for magnetic strip, keys etc. Similarly simplicity, cheapness, ease of implementation and use, the desired characteristics of the password based scheme also explain the waning confidence which designers have in its ability to provide sufficient levels of authentication (Conn A.P et al, 1990). The strength of the system is dependent on the secrecy of the underlying shared secret. Unfortunately this makes the scheme suffer from a fundamental flaw stemming from human psychology. Passwords should be easy to remember and provide swift authentication. On the other hand, in terms of security they should be difficult for an intruder to guess, must consist of a long, random selection of alphanumeric keys, change from time to time and be unique to a single account (Joyce R & Gupta G, 1990). Because of these stringent requirements, people feel the need to choose simple and predictable words or numbers related to everyday life, and engage in insecure practices, such as recording their secret keys close to their authentication device, or even worse, sharing them (Garfinkel S. & Spafford E.H, 1996). The problem is so serious that the user is often considered as the 'weakest link' in the security chain (Leggett J & Williams G, 1988). Furthermore with increase in computing power, it becomes trivial to initiate dictionary and brute force attacks to guess the secret. The increasing need for security in present-day society has boosted the interest for the use of biometrics.
Biometrics, which refers to identifying an individual based on his or her physiological or behavioral characteristics, has the capability to reliably distinguish between an authorized person and an imposter. A biometric is extremely difficult to copy, share, or distribute and is resistant to spoofing unless the biometric data is being transmitted in clear. Hence it provides

stronger defense against non repudiation compared to passwords and tokens which can be easily shared or copied. In addition as no user biometric is easier to break than another, all users are on the same level. The main disadvantage of biometric methods is that they usually require the support of specialized hardware device for their implementation as well as ways for securing the channel over which the biometric data is traveling. This increases highly their installation cost and makes it more difficult to use without proper training in some cases. Moreover if a biometric is compromised or a document is lost, they are not replaceable as are passwords or tokens.

The commonly adopted metrics for biometric system performance are the false rejection rate and the false acceptance rate, which respectively correspond to two popular metrics: sensitivity and specificity (Kung S.Y. et al.2005). Mistaking biometric measurements from two different persons to be from the same person is called *false match*. On the other hand considering two biometric measurements from the same person to be from two different persons is *false reject*. These two popular metrics are often termed as false accept (FA) and false reject (FR) respectively. Authentication schemes can be combined to enhance security and convenience, forming multi-factor authenticator.

The system detailed in the present paper, fuses two security mechanisms in order to reinforce user authentication. It employs a password string complemented with its corresponding keystroke pattern which represents the way a user behaves. The benefits of the keystroke biometric (a two factor authentication) are numerous. Both components need to be present for the user to be authenticated: the password and a "good-enough" keystroke pattern. It provides a distinct, reproducible, and a non obtrusive means of user identification. Being an inexpensive biometric, the only hardware required is a keypad, its implementation and acceptance is expected to be much easier. Keystroke timing values captured when a user is typing his usual password are compared against profile values, and a match, within a certain precision threshold will grant access to the user.

3. RELATED WORK

Since the uniqueness of a user typing pattern was first reported by Joyce and Gupta in 1990 (Joyce R & Gupta G, 1990), work has progressed in using typing behavior as an authentication tool. Some products that use such characteristics are now available on the market e.g. Biopassword (Biopassword, 2006). Unfortunately the effectiveness and inner working of such systems are not known as very little research about these is available in the public domain. Statistical models and digraph latencies were the pioneers for some time and even had two patents issued (Bechtel J. et al.,2002), before now being replaced by methods from machine learning and artificial intelligence. Delving into the details of each approach is beyond the scope of this paper but a few studies stand out in their significance and deserve a mention here as they have stimulated our study.

The typed string length is an important issue and it is expected that misclassification varies with length size (Bleha S & Obaidat M, 1991), (Araújo L.C.F. et al., 2005). In 1990, Joyce and Gupta (Joyce R & Gupta G, 1990) reported their work related to keystroke dynamics. In their system, users need to register reference signatures by typing {user name, password, first name, last name} eight times. Out of the four strings only two target strings were analyzed. In a similar work, Bleha et al, used a 31-character string and a login (Bleha S et al., 1990). In another work the target strings were divided into three difficulty levels. (Coltell O et al., 1999). In 1997, Monrose and Rubin (Monrose F & Rubin A, 1998) extended the basic research by considering a system that uses "free Style" (i.e., nonstructured) text, which is a

few sentences from a list of available phrases. Moreover they applied a clustering method to their system in order to reduce the search time from the database. Later on, Leggett et al. (Leggett J et al., 1991) conducted similar experiments by applying a long string of 537 characters and reported a result of 5.0% FAR and 5.5% FRR. Recently through the use of neural networks, short strings such as real-life names (Brown M & Rogers S.J, 1993), (Obaidat M & Sadoun S, 1997) were investigated. However the latter had three practical limitations in that it included imposter pattern, had a large training data set (6300 from owner and 112 from imposters) which was furthermore not chronologically separated. Some other studies imposed a fixed text string to be typed by all users (for example: "UNIVERSITY OF MISSOURI COLUMBIA" (Bleha D & Obaidat M, 1991). Others have allowed different users to have different strings such as their names and usernames as their passwords. The impact of the constituents of a password was emphasized in a recent study by Araújo et al. (Araújo L.C.F et al.,2005) The choice of a target string with include capital letters, combination of *shift* and *caps lock* keys were found to play an important role in the authentication process. Additionally familiarity of the user with the target string was also investigated in that same study. More recently Revett and Khan (Revett K. & Khan A., 2005) concluded that addition of keyboard partitioning can reduce the impostor success rate (FAR). The keyboard is divided in several regions from which the characters forming the password were selected. This ensured that the right hand, left hand and fingers were all involved in entering the desired text.

An ideal system has to be highly repeatable for the same user and different between different users in terms of keystroke dynamics. With this mindset we embarked on the comparison of different passwords which are in common use. The novelty of this approach is that it acknowledges the fact that, for the enhanced password scheme to be accepted, it has to nullify the difference between the different types of passwords that exist. Random secrets are common for software keys and other situations where users cannot remember their password. Most users, when registering for a service, usually select a password with which they have some familiarity. In other cases the password may be forced on them, derived from a common word for easy recollection. A typical scenario is the password given for the marks entry system at the University of Mauritius. In short three types of password will be investigated, human generated, imposed one and computed generated. The human generated one is the name which they are used to typing on nearly all accounts.

4. SETUP

Capturing keystroke is vital to the operation of the keystroke authentication system developed. For the verifier to work, it is necessary to obtain accurate timing information with sufficient resolution. A toolkit was constructed in Microsoft Visual Basic 6.0 which allowed capturing of key depression, key release and key code for each physical key being used. Feature values were then computed from the information in the raw data file to characterize the template vector of each authorized user based on flight and dwell times recorded to the nearest millisecond. One of the issues encountered with efficient typists was release of a key after s/he has depressed more than one key. The solution for this was to temporarily store all the key events for a login attempt and then to re-order them so that they were arranged in the order they were first depressed. The toolkit implemented allowed collection of data in the background while the user types on the keyboard. Using the password "Thurs1day" we obtained 8 keystrokes interval and 9 keystroke duration times omitting the "Enter" key. To obtain a reference template, we followed an approach similar to that used by the banks and other financial institutions. A new user goes through a session where he/she provides a

number of digital signatures by typing the selected password a number of times. The number of enrollment attempts was chosen to provide sufficient data to obtain an accurate estimation of the user mean digital signature as well as information about its variability. Another point worth consideration was preventing annoyance on behalf of the users when keying the same text too many times. The participants were mostly final year students as well as some members of the staff working in the laboratory - giving a total of 50 participants. Four members did not complete the experiment.

The derived password selected for this experiment was thus "Thurs1day" which met the following considerations. It is referred to as the default password. The sequence length of 9 characters is expected to avoid typing tiredness and consisted of both digits, characters, and a combination of big and small caps as recommended for good passwords. To obtain the computer generated (spontaneous) password the user was asked to press a button to generate a random string of characters which could include a combination of these letters, digits and special symbols. The computer generated string was then subject to the same procedures as the password mentioned above and the user selected a name also. As noted earlier, the identity verifier compares test signature provided by the user wishing to access a computer system with the reference signature stored. According to the degree of match the user is either allowed access or rejected. Typing proficiency was not a requirement in this study. The study was explained to all volunteers and they were given plenty of time to practice with the desired passwords so as to simulate real world environment as far as possible. The aim of the practice was to minimize use of "backspace" and "delete" key as this would produce erroneous values.

5. RESULTS

The numerical values obtained for template creation and login attempt was then passed to the program developed in Matlab for both the learning process and calculation of system parameters. The first step was to explore and fine tune the parameter values for the simple multiple layer perceptron (MLP) with back propagation (BP). The motivation behind using neural network in MLP/BP with a sigmoid transfer function can be found in (Lin D.T, 1997), (Obaidat M. & Macchairolo D.T, 1994). A complete analysis of the model used can be found in the literature (Rumelhart D. et al., 1986) and also (Hwang B & Cho S., 1998).

Figure 1 shows variation of the neural network learning with varying number of hidden nodes. The initial weights and bias were initialized randomly with the error level set to 0.01 and the system was optimized using the default password mentioned above. This clearly indicates that an increase in hidden nodes facilitates learning of the pattern indicate by the near zero error value as depicted by D.T. Lin (Lin D.T, 1997).

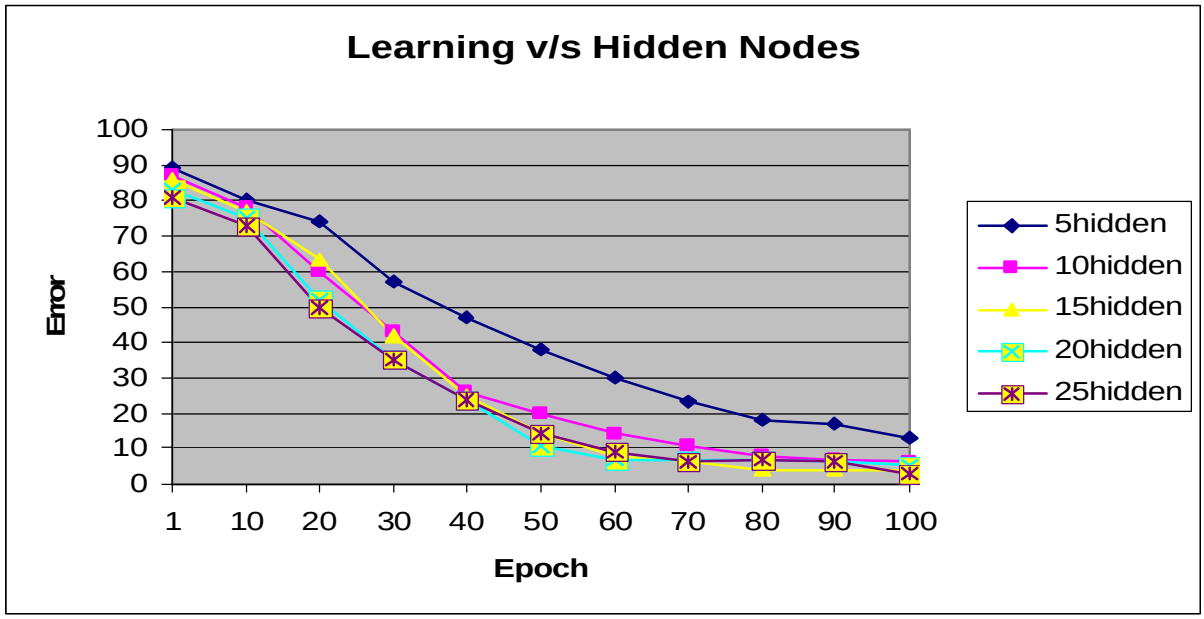

Figure 1. Learning of the MLP/BP model with varying hidden nodes

Figure 2 below depicts the variation of the network with different values of the learning rate, proportion of the error which is propagated backward to alter the weights and bias of the nodes.

An epoch is one complete sweep through all records in the training set by the neural network. More epochs implies more iterations using the same data (more sweeps) for better adjustment to the neural network weights and biases. The line labeled 'd.variable' demonstrates how an increase in the number of inputs nodes improves the performance. From the graph above, 20 epochs only is required to achieve the same performance reached previously by 55 epochs with learning rate of 0.8; all other values remaining constant.

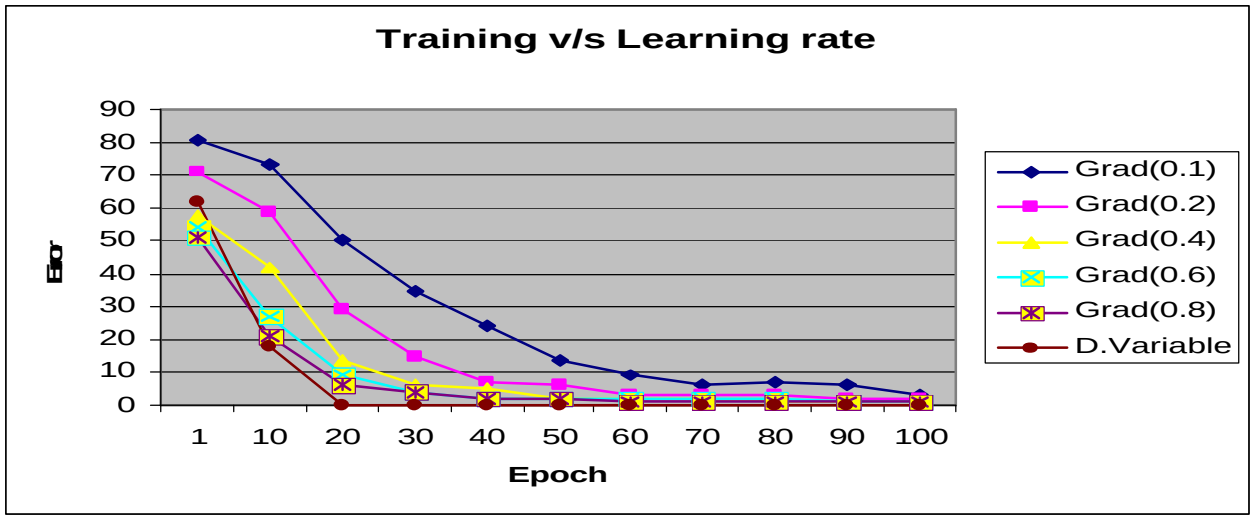

Figure 2. Learning of the MLP/BP model with variation of learning rate

Figure 3 shows how the error percentage in MLP/BP identification decreases as the number of logins used for learning increases. As expected the greater the number of attempts made by the authentic users during learning the easier can the users be identified. As recommended in (Araújo L.C.F et al., 2005) a variation from five to ten samples were considered during learning.

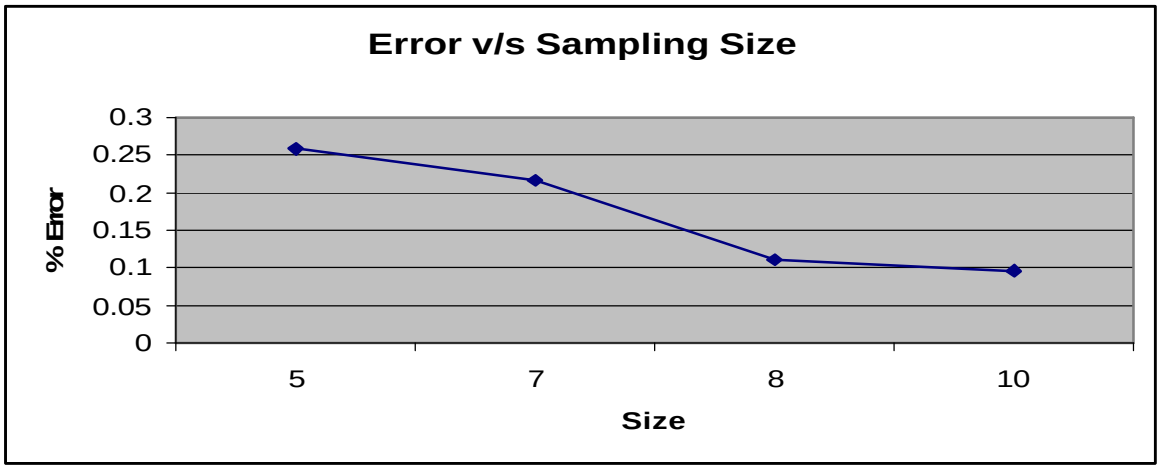

Figure 3. Improvement in system performance with increase in learning sample size.

After having collected the data to be used for building the templates for the different authentic user, the system was left for users to practice. The software allowed computation of attempts made by authentic users as well as those by impostors. Table 1 summarizes the results of the comparison experiments performed using the optimal values obtained above (20 hidden nodes, learning rate of 0.6, sample size of 10 and a threshold of 70 %).

	Default			Spontaneous			Human	
	FAR	FRR		FAR	FRR		FAR	FRR
Authentic Users	3/144	7/144		5/50	10/50		4/300	5/300
Impostors	20/80			2/40			5/300	

Table 1 Password Performance comparison.

As seen in the table above, with the same password being used as a default password, the user was asked to type that specific word and then the keystroke timing captured was matched to the complete database of profiles to find the best match. The same technique was applied to system generated and human generated passwords where each users where asked to type some names including his/her own name. For impostors' attempts the second column has been left clear since impostor attempts are either erroneously accepted or correctly rejected. While the results obtained for human selected passwords are broadly in line with those obtained in previous studies, Table 1 seems to favor the use of human generated (names) password for keystroke dynamics. The important finding is that for computer generated passwords, the user types differently hence risk of impersonation is minimized but this increases its vulnerability to sholder surfing. This deduction about the uniqueness of each attempt is furthermore supplemented by a high rejection rate for authentic users. Moreover, though the users made a large number of attempts only a few were valid ones as they pressed the "Backspace and Delete" keys a number of times with usual breaks to think and decide what to type. The default password being derived from a common word in English it has intermediate performance. This supports the statement that users have a more representative profile when they type what they are familiar with.

6. CONCLUSION AND FUTURE WORK

Surrogate representations of identity such as the commonly used password mechanism and possession based control (prevalent in banking and government applications) no longer suffice. In that context we have presented our study on a technique which, even when user A shares password with user B, will still deny access to B unless he is capable of mimicking the keystroke dynamics of A. Since stable biometric signals are difficult to replace when compromised, we have investigated an alterable multifactor authentication method which can be easily, as well as cheaply, incorporated into actual systems while still being unobtrusive. In any system incorporating a keypad/keyboard, the user will be pressing keys and therefore these keypresses and releases can be made use of. Nowadays, with the explosion of online systems, these keystroke timings can be securely transferred from the keypad to the authentication device with the text typed.. However transferring the inherent keystroke timing in plain over the internet can lead to other security breaches. In that same line of thought we have to ascertain ourselves that the captured keystroke are really from the claimed user and no impersonation or inserted fake data is being captures. Therefore in addition to correctness of the entered matching of the timing vectors also can be performed.

Although previous research work has favored the use of neural networks, our work has shown some major limitations which should be solved before widespread acceptability is achieved. An authentication system has to be instantaneous for it to achieve widespread use, therefore the time required for training and processing the input are crucial. Any implementation should not delay the response of the current password mechanism and this was not the case for our prototype system. Clearly as the number of nodes and variables increases, the algorithm slows down the system response time. The hardened password mechanism may increase user frustration. Keystroke dynamics do not integrate seamlessly with textual passwords.

The experiments performed show that the results reported cannot be generalized for different types of password. Moreover in cases where the user has forgotten his password, a system based on keystroke dynamics may fail, when the user types a system-generated one. Additionally this shows that habituation/familiarity of the keyed string impacts on the performance. This raises the issue of having to change the stored template for the user after a period of use of the system.

In this project we have used both the inter-key and key press time as independent features. Incidentally paying attention to their combination or even to the selection of a few features only will, we feel, yield better results. Similarly variation of system performance with different threshold values as well as with an increase in the number of attempts remains an avenue to be explored. The quantum of attempts before template update remains a challenge in this field.

In this paper have trained the neural network with the default password and then use the same parameters in order to evaluate the performance of the other types of password. Clearly this has had an impact on the performance. Similarly the sample size also does affect the performance neglecting the practical aspect that users have made more errors/omissions for the spontaneous password. .

To have an acceptable level of performance for experiments of this kind, it is necessary to take into account elements such as the general state or condition of the subjects, the specific activity, and the context in which the activity is performed (Bailey R.W,1982). A personal laptop was reserved exclusively for this but still improvement is feasible in that direction. Similarly in all experiments we have considered results where the text has been introduced correctly after the users were informed what to type. Clearly implementations which allow for user corrections remain an interesting avenue to consider.

7. ACKNOWLEDGEMENTS

I would like to show my appreciation to all the users who happily participated in my experiments and hope to be able to rely on them for the coming ones also. Finally I express my gratitude to the anonymous referees for their interesting comments, suggestions and for providing constructive criticisms on the first draft of this paper.

8. REFERENCES

(Araújo L.C.F. et al.,2005) . Lívia C. F. Araújo, Luiz H. R. Sucupira Jr., Miguel G. Lizárraga, Lee L. Ling, and João B. T. Yabu-uti, User "Authentication through Typing Biometrics Features", IEEE Transactions on Signal Processing, Vol 53 N0. 2, February 2005, pp 851-855.

(Bailey R.W,1982) R. W. Bailey, Human Performance Engineering. Englewood Cliffs, NJ: Prentice-Hall, 1982.

(Bechtel J. et al.,2002) J.Bechtel, G.Serpen and M. Brown, International Journal of Computer Intelligence and Applications Vol 2 No.2 pp 1-22, 2002.

(Biopassword,2006) http://www.biopassword.com.Accessed on the 28th December 2006.

(Bleha S & Obaidat M, 1991) Bleha and M. Obaidat, , "Dimensionality reduction and feature extraction applications in identifying computer users," IEEE Trans. Syst., Man, Cybern., Vol. 21,no. 2, pp. 452-456, 1991

(Bleha S et al.,1990) Bleha, S., Slivinsky, C., Hussain, B. "Computer-Access Security Systems Using Keystroke Dynamics". IEEE Trans. Pattern Anal. Machine Intell., Vol. 12, No. 12, pp 1217-1222,1990

(Bolle R ,2003) R. Bolle. Guide to Biometrics. Springer-Verlag, 1st edition, December 2003.

(Brown M & Rogers S.J, 1993), Brown M, Rogers SJ: "User identification via keystroke characteristics of typed names using neural networks", Int J Man Machine Stud, Vol 39, pp 999-1014, 1993

(Coltell O et al.,1999) Coltell, O., Badfa, J.M., Torres, G.:" Biometric Identification System Based in Keyboard Filtering". Proceedings IEE 33rd Annual 1999 International Carnahan Conference on Security Technology.pp 203-209, 1999.

(Conn A.P et al.,1990) A.P. Conn, J.H. Parodi, and M. Taylor, "The Place of Biometrics in a User Authentication Taxonomy," Proc. 13th National Computer Security Conf., NIST. Computer Security Center, Gaithersburg, 990.

(Garfinkel S. & Spafford E.H,1996) S. Garfinkel and E. H. Spafford. Practical UNIX Security. OReilly, 2nd edition, April 1996.

(Hsu R et al.,2002) R. Hsu, M. Abdel-Mottaleb, and A. Jain. "Face detection in color images". IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 25(5),pp 696–706, 2002.

(Hwang B & Cho S.,1998). B. Hwang and S. Cho, " Output Characteristics of autoassociative MLP and its application in novelty detection. " Proc of Korea Information Science society vol 25 no 11 pp

581-583, 1998.

(Jobusch D.L & Oldehoeft A.E,1989) D.L. Jobusch and A.E. Oldehoeft, "A Survey of Password Mechanisms: Weaknesses and Potential Improvements, Part 1," Computers & Security,Vol. 8, 1989, pp. 587–604.

(Joyce R & Gupta G,1990) Rick Joyce and Gopal Gupta, "Identity Authentication Based on Keystroke Latencies", Vol 33 (2) Communications of the ACM pp168-176, 1990

(Kung S.Y. et al.2005) S. Y. Kung, M. W. Mak, S. H. Lin, Biometric Authentication, New Jersey: Prentice Hall, 2005

(Leggett J & Williams G, 1988) Leggett, J., and Williams, G. "Verifying identity via keyboard characteristics". Int. J. Man-Machine Studies 23, 1 (Jan. 1988), pp 67-76.

(Leggett J et al.,1991) Leggett J, Williams G, Usni M, Long M]. Dynamic identity verification via keystroke characteristics. Int J Man Machine Stud ,Vol 35 pp 859-870, 1991;

(Lin D.T,1997) D.T.lin: "Computer Access authentication with neural network based keystroke indentity verification", Proc IEEE Intl Conf Neural Networks pg 174-178, 1997

(Mandujano S & Soto R,2004) S. Mandujano and R. Soto: "Deterring Password Sharing: User Authentication via Fuzzy c-Means Clustering Applied to Keystroke Biometric Data ",Proceedings of the Fifth Mexican International Conference in Computer Science (ENC'04),2004

(Monrose F & Rubin A,1998)]. F. Monrose and A. Rubin. Authentication via Keystroke Dynamics. 4th ACM Conference on Computer and Communcations Security, p 48-56,1998.

(Obaidat M & Sadoun S,1997) Obaidat M, Sadoun S. Verification of computer users using keystroke dynamics. IEEE Trans Syst Man Cybernet Part Vol 27 (2)pp 261-269,1997

(Obaidat M. & Macchairolo D.T,1994) M.S. Obaidat and D.T Macchairolo, "A multilayer neural network system for computer access security", IEEE transactions on Systems, Machine and Cybernetics VOl 24, No 5, May 1994.

(Pfleeger C.P, 1997). Pfleeger, CP, 1997, "Security in Computing International Edition Second Edition, Prentice Hall International, Inc, Upper Saddle River, NJ, 2nd edition, 1997

(Pfleeger C.P,1993) C.P. Pfleeger, Security in Computing, Prentice - Hall, Upper Saddle River, N.J., 1993.

(Revett K. & Khan A., 2005) Kenneth Revett, Aurangzeb Khan, Revett, K. and Khan, A., 2005, "Enhancing login security using keystroke hardening and keyboard gridding", Proceedings of the IADIS MCCSIS pp 1-6, 2005.

(Roland,2004) Roland, J. CCSP Self-study: Securing Cisco IOS networks (SECUR). Indianapolis, IN: Cisco Press, 2004.

(Ru W.G and Eloff J.H.P , 1993). W.G. de Ru and J.H.P. Eloff, "Improved Password Mechanisms through Expert System Technology," Proc. Ninth Ann. Computer Security Applications Conf., IEEE Computer Society Press, Los Alamitos, Calif., pp. 272–280, 1993,

(Rumelhart D. et al.,1986) D. Rumelhart. G. Hnton and R. Williams " Learning internal representations by error backpropagation,, " In parallel

distributed processing Cambridge, MA, pp 318-362, MIT press 1986.

(Spender J.C,1987) J.C. Spender, "Identifying Computer Users with authentication Devices (Tokens)," Computers & Security, Vol. 6, pp. 385–395, 1987,