International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-1, January 2016
ISSN: 2395-3470
www.ijseas.com

Biometric Authentication Techniques: A Study on Keystroke Dynamics

Sandhya Avasthi
Assistant Professor, Krishna Engineering College
Tanushree Sanwal
Assistant Professor, Krishna Engineering College

***Abstract*— Biometrics technologies are gaining popularity today since they provide reliable and efficient means of authentication and verification. Our dependency on electronic devices is growing, and so is our need to secure information on them. Keystroke Dynamics is one of the famous biometric technologies, which identifies the authenticity of a user when the user is working via a keyboard. The authentication process is done by observing the variation in the typing pattern of the user. A comprehensive study of the existing keystroke dynamics methods, metrics, and different approaches are presented. This paper also discusses about the various security issues and challenges faced by keystroke dynamics.**

Keywords- Biometrics, Keystroke Dynamics, computer Security, Information Security, Biometric Authentication.

1. INTRODUCTION

Preventing unauthorized access or restricting access to information system is first step towards security, which is possible through user Authentication. User authentication is the process of verifying identity of the user. The authentication is accomplished by matching some short-form indicator of identity, such as a shared secret that has been pre-arranged during enrollment or registration for authorized users. This is done for the purpose of performing trusted communications between parties for computing applications.

User authentication is categorized into three categories [17]:

1. Knowledge - based,
2. Object or Token - based,
3. Biometric - based.

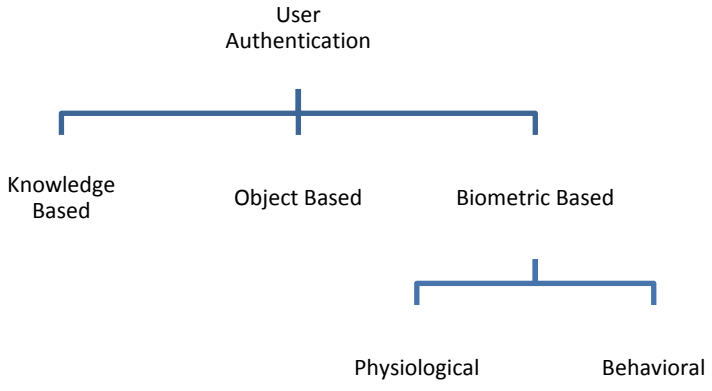

Figure 1

Figure1. Shows classification of user authentication method. The knowledge-based authentication is characterized by secrecy and depends on information someone knows. The examples of knowledge-based authenticators are commonly known passwords and PIN codes. The object-based behavioral characteristics are related to what a person does, or how the person uses the body. Voiceprint, gait Traditional keys to the doors can be assigned to the object based category. Usually the token-based approach is combined with the knowledge-based approach. An example of this combination is a bankcard with PIN code. In knowledge-based and object-based approaches, passwords and tokens can be forgotten, lost or stolen. They have several usability limitations associated with them. For instance, managing multiple passwords / PINs, and memorizing and recalling strong passwords are not easy tasks. Biometric-recognition overcomes such difficulties of knowledge-based and object based approaches.

Biometric technologies are automated methods of verifying or recognizing the identity of living person based on physiological or behavioral characteristics [2]. The characteristics used for biometric purposes can be divided into physiological and behavioral types [17]. ***Physiological characteristics*** refer to physical characteristics of a certain part of the body or inherent traits of a person. Examples are Fingerprints, Hand Geometry, Vein Checking, Iris Scanning, Retinal Scanning, Facial Recognition, and Facial Thermogram.

Behavioural characteristics are related to what a person does, or how the person uses the body like voiceprint, gait recognition, Signature Recognition, Mouse Dynamics and keystroke dynamics. A very important behavioural pattern is typing, which is referred to as ***Keystroke Dynamics***. When a person types, the time delay between successive keystrokes, keystroke durations, finger position and applied pressure on the keys can be used to construct a unique signature (i.e., profile) for that individual. Keystroke dynamics is considered as a strong behavioural Biometric based Authentication system [1]. It is a process of analyzing the way a user types at a terminal in order to identify the users based on typing rhythm and speed patterns. The raw measurements used for keystroke dynamics are dwell time and flight time. *Dwell time* is the time duration that a key is pressed and *Flight time* is the time duration in between releasing a key and pressing the next key.

While typing a sequence of characters, the time a person need to find the right key (flight time) and the time he holds down a key (dwell time) is unique to each individual and can be calculated. Overall typing speed is independent of these parameters. The rhythm is person dependent when it comes to typing sequence of characters. For example someone used to typing in English will be quicker at typing certain character sequences such as 'the' than a person with *Hindi* roots or *Telgu* roots.

Keystroke Dynamics is good for logical access control for many reasons:-

- This biometric system does not necessitate any additional sensor.
- User acceptability is high as it is natural for everybody to type a password for authentication purposes.
- This system respect the privacy of users if the biometric template of an individual has been stolen the user just has to change its password.

2. IDENTIFICATION AND VERIFICATION

Keystroke dynamics systems can run in two different modes [2] namely the ***Identification mode*** and ***Verification mode***. Identification is the process of trying to find out a person's identity by examining a biometric pattern calculated from the person's biometric features. A larger amount of keystroke dynamics data is collected, and the user of the computer is identified based on previously collected information of keystroke dynamics profiles of all users. For each of the users, a biometric template is calculated in this training stage. A pattern that is going to be identified is matched against every known template, yielding either a score or a distance describing the similarity between the pattern and the template. The system assigns the pattern to the person with the most similar biometric template. To prevent impostor patterns (in this case all patterns of persons not known by the system) from being correctly identified, the similarity has to exceed a certain level. If this level is not reached, the pattern is rejected. Identification with keystroke dynamics means that the user has to be identified without additional information besides measuring his keystroke dynamics.

A person's identity is checked in the verification case. The pattern that is verified is only compared with the person's individual template. Keystroke verification techniques can be classified as either static and dynamic or continuous [22]. Static verification approaches analyze keystroke verification characteristics only at specific times providing additional security than the traditional username/password. For example, during the user login sequence, Static approaches provide more robust user verification than simple passwords but the detection of a user change after the login authentication is impossible. Continuous verification, on contrary, monitors the user's typing behavior throughout the course of the interaction. In the continuous process, the user is monitored on a regular basis throughout the time he/she is typing on the keyboard, allowing a real time analysis [21]. It means that even after a successful login, the typing patterns of a person are constantly monitored and when then do not match user profile, access to the system is blocked.

3. METHODS AND METRICS FOR KEYSTROKE DYNAMICS

Data acquisition techniques and typing metrics upon which keystroke analysis can be based have been studied in papers [3, 5, 7, 10, 15]. The techniques for verifications are either static or continuous. In static verification approach keystroke verification is done only at specific times, for example, when a person is doing login sequence. User verification through static approach is better than simple passwords, but do not provide security after login is done. On the other side, continuous verification monitors the user's typing behavior throughout the whole interaction. The following section summarizes the basic methods and metrics that can be used.

Static at login– In static keystroke analysis method a typing pattern based on a known keyword, phrase or some other predetermined text is authenticated. During system enrollment process the typing pattern is captured and compared against previously recorded patterns.

Periodic dynamic– Dynamic keystroke analysis authenticates a user on the basis of their typing during a **logged session**. The data, which is captured in the logged session, is then compared to an archived typing pattern to determine the deviations. In a periodic configuration, the authentication can be constant; either as part of a timed supervision.

Continuous dynamic– Continuous keystroke analysis extends the data capturing to the entire duration of the logged session. The continuous nature of the user monitoring offers significantly more data upon which the authentication judgment is based. Furthermore, an impostor may be detected earlier in the session than under a periodically monitored implementation.

Keyword-specific– Keyword-specific keystroke analysis extends the continuous or periodic monitoring to consider the metrics related to specific keywords. Extra monitoring is done to detect potential misuse of sensitive commands. Static analysis could be applied to specific keywords to obtain a higher confidence judgment.

Application-specific– Application-specific keystroke analysis further extends the continuous or periodic monitoring. It may be possible to develop separate keystroke patterns for different applications. In addition to a range of implementation scenarios, there are also a variety of possible keystroke metrics. The Following are the metrics widely used by keystroke dynamics.

Digraph latency– Digraph latency is the metric that is most commonly used and it typically measures the delay between the key-up and the subsequent key-down events, which are produced during normal typing (e.g. pressing letter T-H).

Tri-graph latency– Tri-graph latency extends the digraph latency metric to consider the timing for three successive keystrokes (e.g. pressing letter T-H-E).

Keyword latency– Keyword latencies consider the overall latency for a complete word or may consider the unique combinations of digraph / trigraphs in a word-specific context.

4. PERFORMANCE MEASURES

Performance of Keystroke analysis is typically measured in terms of various error rates [13], namely False Accept Rate (FAR) and False Reject Rate (FRR). FAR is the probability of an impostor posing as a valid user being able to successfully gain access to a secure system. In statistics, this is referred to as a Type II error. FRR measures the percent of valid users who are Keystroke Dynamics-based Authentication rejected as impostors. In statistics, this is referred to as a Type I error. Both error rates should ideally be 0%. From a security point of view, type II errors should be minimized that is no chance for an unauthorized user to login. However, type I errors should also be infrequent because valid users get annoyed if the system rejects them incorrectly. One of the most common measures of biometric systems is the rate at which both accept and reject errors are equal. This is known as the Equal Error Rate (EER), or the Cross-Over Error Rate (CER). The value indicates that the proportion of false acceptances is equal to the proportion of false rejections. The lower the equal error rate value, the higher the accuracy of the biometric systems.

5. SECURITY OF KEYSTROKE DYNAMICS

So far, very little research has been conducted to analyze keystroke dynamics concerning security [4]. The application of keystroke dynamics to computer access security is relatively new and not widely used in practice. Keystroke dynamics schemes are analyzed regarding traditional

attack techniques in the following section. The traditional attacks can be classified as: Shoulder Surfing, Spyware, Social Engineering, Guessing, Brute Force and Dictionary Attack.

Shoulder Surfing A simple way to obtain a user's password is to watch them during authentication. This is called shoulder surfing. No matter if keystroke dynamics are used in the verification or identification mode, shoulder surfing is no threat for the authentication system. Password is not used in the identification case and therefore the password cannot be stolen. Only the keystroke pattern is important and decisive. In case of verification, an attacker may be able to obtain the password by shoulder surfing. However, keystroke dynamics for verification is a two-factor authentication mechanism. The keystroke pattern still has to match with the stored profile.

Spyware Spyware is software that records information about users, usually without their knowledge. Spyware is probably the best and easiest way to crack keystroke dynamic-based authentication systems. If a user unintentionally installs a Trojan which records all of the user's typing, keystroke latencies and keystroke durations an attacker can use this information to reproduce the user's keystroke pattern. A program could simulate the user's typing and get access to the system from the keystroke pattern. Much more research in the area is expected.

Social Engineering Social engineering is the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick people into revealing sensitive information or getting them to do something that are against typical policies. Using this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes. Phishing is social engineering via e-mail or other electronic means. On first sight, social engineering is not possible with keystroke dynamics. In the identification case there is no password that can be given away, not even on purpose. Asking for the password on the phone and pretending to be the authorized user, is not feasible. Nevertheless, phishing, social engineering via Internet, may be a way of tricking a user togive away his keystroke pattern. The attacker might portraitas a trustworthy person, asking the user to log-on to a primed website. When the user logs-on to the website the attacker might record the keystroke rhythm of the users. However, the success rate would probably be very low. The user must type his username and password several times in order to have a meaningful keystroke pattern.

Guessing People use common words for their passwords. The way of typing of a different user can hardly be simulated. There are just too many varieties of ways of typing on the keyboard. Guessing of typing rhymes is impossible in keystroke dynamics.

Brute Force In a brute force attack, an intruder tries all possible combinations of cracking a password. The more complex a password is, the more secure it is against brute force attacks. The main defense against brute force search is to have a sufficiently large password space. The password space of keystroke dynamic authentication schemes is quite large. It is nearly impossible to carry out a brute force attack against keystroke dynamics. The attack programs need to automatically generate keystroke patterns and imitate human input. If keystroke dynamics are used in a two-factor authentication mechanism, that is password and keystroke, it is almost impossible to overpower the security system.

Dictionary Attack A dictionary attack [4] is a technique for defeating authentication mechanism by trying to determine its pass phrase by searching a large number of possibilities. In contrast to a brute force attack, where all possibilities are searched through exhaustively, a dictionary attack only tries possibilities that are most likely to succeed, typically derived from a list of words in a dictionary. With brute force searches, it is impractical to carry out dictionary attacks against keystroke dynamic authentication mechanisms. It is possible to use a dictionary attack which consists of general keystroke patterns, but an automated dictionary attack will be much more complex than a text based dictionary attack. Again the attack programs need to automatically generate keystroke patterns and imitate human input. Overall keystroke dynamics are less vulnerable to brute force and dictionary attacks than text based passwords.

6. CHALLENGES

Keystroke dynamics is a behavioral pattern exhibited by an individual while typing on a keyboard [21]. User authentication through keystroke dynamics is appealing for many reasons such as:

(i) It is not intrusive, making it quite applicable to computer access security as users will be typing at the keyboard anyway.

(ii) It is relatively inexpensive to implement, since the only hardware required is the computer [12].

Unlike other physiological biometrics such as fingerprints, retinas, and facial features, all of which remain fairly consistent over long periods of time, typing patterns can be rather erratic. Even though any biometric can change over time, typing patterns have smaller time scale for changes. Not only the typing pattern is inconsistent when compared to other biometrics, a person's hands can also get tired or sweaty after prolonged periods of typing. This often results in major pattern differences over the course of a day. Another substantial problem is that typing patterns vary based on the type of the keyboard being used, the keyboard layout (i.e. QWERTY), whether the individual is sitting or standing, the person's posture if sitting, etc. The fact is that the distributed nature of keyboard biometrics also means that additional inconsistencies may be introduced into typing pattern data.

7. CONCLUSION

Biometric technologies and its future scope are wide. Devices and applications will depend hugely on biometric technology for security worldwide. There are several factors that will push the growth of biometric technologies. A major inhibitor of the growth of biometrics has been the cost to implement them. Moreover, increased accuracy rates will play a big part in the acceptance of biometric technologies. The development and research into biometric error testing false reject (false non-match) and false accept (false match), has been of keen interest to biometric developers. Keyboard Dynamics, being one of the cheapest forms of biometric, has great scope. In this paper an effort has been taken to give the existing approaches, security and challenges in keystroke dynamics in order to motivate the researches to further come with more novel ideas

REFERENCES

[1] Ahmed Awad E. Ahmed, and IssaTraore, "Anomaly Intrusion Detection based on Biometrics", Proceedings of the IEEE, 2005.

[2] Anil K. Jain, Arun Ross and Salil Prabhakar2, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.
[3] Attila Meszaros, Zoltan Banko, Laszlo Czuni, "Strengthening Passwords by Keystroke Dynamics", IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems:Technology and Applications, 6-8, September 2007.
[4] Benny Pinkas ,"Securing Passwords Against Dictionary Attacks",CCS'02, 18–22,November 2007.
[5] Bergando et al, "User Authentication through keystroke Dynamics", ACM transaction on Information System Security" Vol.No. 5, pg367-397, Nov 2002.
[6] Brown, M., Rogers, J. , "User Identification via Keystroke Characteristics of Typed Names using Neural Networks".International Journal of Man-Machine Studies, vol. 39, pp. 999-1014,1993
[7] Cho et al , "Web based keystroke dynamics identity verification usingneural network", Journal of organizational computing and electronic commerce, Vol. 10, No. 4, 295-307, 2000.
[8] Clarke, N. L. and Furnell, S.M., 'Authenticating mobile phone usersusing keystroke analysis' International Journal of Information Security, 6 (1): 1-14, 2007.
[9] Downland, P. and Furnell, S., "A long-term trail of keystrokeprofiling using digraph, trigraph and keyword latencies", in proceedings of IFIP/SEC 19th International Conference onInformation Security, pages 275-289,2004.
[10] Enzhe Yu, Sungzoon Cho, "Keystroke dynamics identity verificationand its problems and practical solutions", Computers & Security,2004.
[11] Glaucya C. Boechat, Jeneffer C. Ferreira, and Edson C. B. Carvalho, Filho, "Using the Keystrokes Dynamic for Systems of Personal Security", Proceedings Of World Academy Of Science, Engineering And Technology, Volume 18 December 2006.[12] Gunetti and Picardi, " Keystroke analysis of free text", ACM Transactions on Information and System Security, volume 8, pages312–347, 2005.
[13] Guven, A. and I. Sogukpinar, "Understanding users' keystroke patterns for computer access security", Computers & Security, 22,695–706, 2003.
[14] Hyoungjoo Lee, Sungzoon Cho, "Retraining a keystroke dynamics based authenticator with impostor patterns", Computers & Security,26(4): 300-310, 2007
[15] John A. Robinson, Vicky M. Liang, J. A. Michael Chambers, and Christine L. Mac Kenzie, "Computer User verification Using Login String Keystroke Dynamics", IEEE transactions on systems, man, and cybernetics—part a: systems and humans, Vol. 28, No. 2, March1998.
[16] Joyce R., Gupta, G., "Identity Authentication Based on Keystroke Latencies", Communications of the ACM, vol. 39; pp 168-176, 1990.
[17] Lawrence O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Proceedings of the IEEE, Vol.91, No. 12, Dec, pp. 2019-2040, 2003.
[18] Leggett, J., Williams, G., Usnick, M., "Dynamic Identity Verification via Keystroke Characteristics". International Journal of Man-Machine Studies, 1991.
[19] Mohammad S. Obaidat, Balqies Sadoun, "Verification of computer users using keystroke dynamics", IEEE Transactions on Systems,Man, and Cybernetics, Part B 27(2): 261-269, April 1997.
[20] Monrose, F., Reiter, M., Wetzel, S, "Password Hardening Based on Keystroke Dynamics", International journal of Information security,1-15, 2001.
[21] Monrose, F., Rubin, A., "Authentication via Keystroke Dynamics",Proceedings of the 4th ACM Conference on Computer and Communications Security, p 48-56, April 1997.
[22] Monrose, R., Rubin, A., "Keystroke Dynamics as a Biometric forAuthentication". Future Generation Computer Systems, 16(4) pp 351-359, 1999.