ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 2, Issue 5: Page No. 62-67

Review of Keystroke Dynamics Technology Used in Mobile Security

Prof. D. N. Rewadkar

Department of Computer Engineering, RMD Sinhgad College of Engineering, Pune, India

dnrewadkar@sinhgad.edu

Dnyaneshwari S. Dhundad

Department of Computer Engineering, RMD Sinhgad College of Engineering, Pune, India

dsdhundat@gmail.com

ABSTRACT
Today Biometrics technologies are achieving more popularity because it provides reliable and efficient means of Verification and Authentication. Keystroke Dynamics is one of the most famous biometric technologies, which is used to identify the identity of the user when user is working via a keyboard. The verification process is done by observing the changes in typing pattern of the particular user. The complete survey of the existing keystroke dynamics techniques, metrics and different approaches are given in this study. This paper also discuss about the various security issues and challenges faced by keystroke dynamics.

Key words: Biometric, Behavioral biometrics, Keystroke Dynamics, computer Security, Information Security, User Verification.

INTRODUCTION:

The primary step in preventing unauthorized access is user Verification. User verification is the process of validating claimed identity. The verification is accomplished by matching some short-form indicator of personality, such as a shared clandestine that has been pre-arranged during enrollment or registration for authorized users. This is usually done for performing trusted communications between the parties for various computing applications. Biometric technologies [1] are defined as automated techniques of conforming the identity of a living person based on physiological or behavioral characteristics.

A)Types of Biometrics technologies

The different types of Biometrics technologies are achieving popularity due to the reason that when used in conjunction with traditional techniques of verification, they provide an extra level of security. Different types of biometrics are widely used for verification.

Biometrics can be classified into two categories: Physiological biometrics and Behavioural biometrics.

1) Physiological biometric*:* identifies the user based on physiological characteristics, such as fingerprints and eye retina/iris scanning. Implementation of physiological biometrics requires additional tools which lead to an increase in costs.

2) Behavioral biometrics*:* captures the behavioral characteristics of the person, such as signature, voice, keystroke dynamics. Keystroke Dynamics is inexpensive to implement because typing pattern of a person can be recorded by using existing systems keyboard.

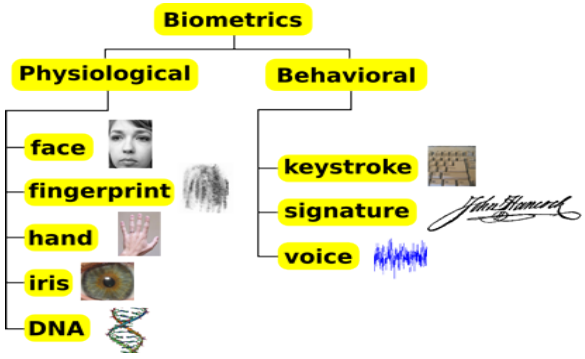

Figure 1: Classification of biometrics

Keystroke dynamics or typing dynamics [3] is the process of analyzing the way a user types at a terminal. This is done by validating keyboard inputs thousands of times per second and try to identify them based on habitual rhythm patterns in the way they type. It is the complete timing information when each key was pressed and when it was released as a person is typing at a keyboard. The behavioral biometric of Keystroke Dynamics is the manner and rhythm in which the person types characters. The unique biometric templates of the user typing patterns are developed by measuring keystroke rhythms, which is used for future verification. Raw measurements available from every keyboard can be recorded to determine Dwell time (the time a key pressed) and Flight time (the time between "key up" and the next "key down"). Key hold time (dwell time) [2] is defined as the time for which each key was pressed and Keystroke latency is the combination of the hold and flight times.

B. Keystroke Verification Techniques

In verification the system verifies how a person types. Keystroke verification techniques [4] can be categorized as either static or continuous.

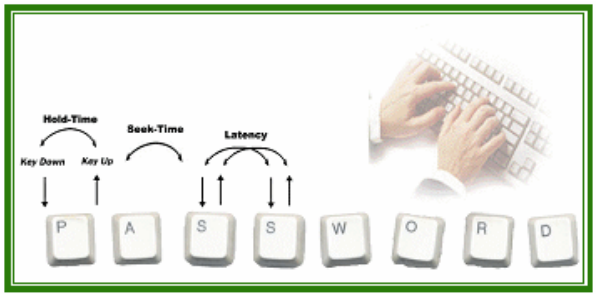

Figure 2: Keystroke dynamics

1) Static verification: This approach study keystroke characteristics at a specific time.

2) Continuous verification: This examines the typing behavior of user throughout the interaction time. Time-features can be taken from keystroke data in many ways, such as studying keystroke latency, interval of key hold, pressure of keystroke, frequency of word errors, and typing rate. However, all of these techniques are not widely used.

Keystroke solutions are generally measured in three ways:

1. dwell time – how long a key is pressed,
2. flight time – how long it takes to move from one key to another and
3. The key code.

The recorded keystroke timing data is then processed through neural algorithm, usually multilayer perceptron network (MLP) and radial basis function (RBF) are used, which determines a primary pattern for future comparison. Vibration information may also be used to create a pattern for future use in both classification and verification tasks. Data needed to analyze keystroke dynamics is achieved by keystroke logging.

II. REVIEW OF CLASSIFICATION AND VERIFICATION

Keystroke dynamics systems works in two different forms [6] namely the Classification type or Verification type. Classification is the process of trying to find out a person's identity by authentication a biometric pattern calculated from the person's biometric features. A large amount of keystroke dynamics data is gathered, and on the basis of previously gathered information of keystroke dynamics profiles of all users, the user of the computer is identified. In this training stage a biometric templates for each user is calculated. The pattern which has to identify is matched against every known template, giving either a score or a distance describing the similarity between the pattern and the template. The pattern is assigned to the person with the most similar biometric template by the system. In order to prevent fraud patterns from being correctly identified (in this case all patterns of the person are not known to the system) the similarity has to exceed a certain level. The pattern is rejected if this level is not reached. Classification 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 person template. Keystroke verification techniques can be classified as either static and dynamic or continuous. Static verification approaches provides extra security by analyzing keystroke verification characteristics only at specific times than 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 verification is impossible. Continuous verification, on contrary, examines the user's typing behavior throughout the course of the interaction. In the continuous process, the user is examined on a regular basis throughout the time he/she is typing on the keyboard, allowing a real time analysis. It means that even after a successful login, the typing patterns of a person are constantly analyzed and when they do not match the user's profile, access to the system is blocked.

III. REVIEW OF TECHNIQUES USED IN KEYSTROKE DYNAMICS

Earlier studies [7], [8], [13], [9] have identified a selection of data acquirement techniques and typing metrics upon which keystroke analysis can be based. The following section sum ups the basic techniques and metrics that can be used.

A)Static login – Static login keystroke analysis authenticates typing patterns which are based on keywords known, predetermined text or phrase. The typing pattern captured is compared with earlier recorded typing patterns stored during system enrollment.

B)Periodic dynamic –Periodic keystroke dynamic analysis authenticates a user on the basis of their typing during a logged session. Data which is captured during the logged session is then compared to an archived typing pattern to determine the deviations. In a periodic configuration, the verification can be constant, either as part of a timed administration.

C)Continuous dynamic – Continuous dynamics analysis extends the data capturing to the complete interval of the logged session. The continuous nature of the user authentication offers significantly more data upon which the verification judgment is based. Furthermore, the fraud may be detected earlier in the session than under a periodically examined implementation.

D)Keyword-specific– Keyword-specific keystroke analysis extends the continuous or periodic examining to consider the metrics related to specific keywords. Extra examining is done to detect potential misuse of sensitive commands.

E)Application-specific–Application-specific keystroke analysis further extends the continuous or periodic examining. It may be possible to build up separate keystroke patterns for different applications.In addition to a range of implementation scenarios, there is also a variety of possible keystroke metrics, the following are the metrics widely used by keystroke dynamics.

F)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).

G)Trigraph latency– Trigraph latency extends the digraph latency metric to consider the timing for three successive Keystrokes (e.g. pressing letter T-H-E).

H) 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.

IV. REVIEW OF PERFORMANCE MEASURE

Performance of Keystroke analysis is typically measured in terms of various error rates [14], called False Accept Rate (FAR) and False Reject Rate (FRR). FAR is the probability of imposter posing as a valid user being able to successfully achieve access to a secured system. In statistics, this is referred to as a Type II error. FRR measures the percent of valid users who are rejected as imposters. This statistics 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 proportion of false acceptances is equal to the proportion of false rejections is indicated by these values. Lower the equal error rate value higher the accuracy of the biometric systems

Table 1: Approches in keystroke analysis

Study	Classification Technique		Users	FAR (%)	FRR (%)
Joyce & Gupta (1990) [16]	Static	Statistical	33	0.25	16.36
Leggett et al. (1991) [18]	Dynamic	Statistical	36	12.8	11.1
Brown & Rogers (1993) [6]	Static	Neural Network	25	0	12.0
Bleha & Obaidat (1993) [27]	Static	Neural Network	24	8	9
Napier et al (1995) [23]	Dynamic	Statistical	24	3.8 (Combined)	
Obaidat &Sadoun (1997) [19]	Static	Statistical	15	0.7	1.9
		Neural Network		0	0
Monrose& Rubin (1999) [22]	Static	Statistical	63	7.9 (Combined)	
Cho et al. (2000) [7]	Static	Neural Network	21	0	1
Ord & Furnell (2000) [25]	Static	Neural Network	14	9.9	30
Bergadano et al. (2002) [5]	Static	Statistical	154	0.01	4
Guven & Sogukpinar(2003) [13]	Static	Statistical	12	1	10.7
Sogukpinar & Yalcin(2004) [28]	Static	Statistical	40	0.6	60
Dowland & Furnell (2004) [9]	Dynamic	Neural Network	35	4.9	0
Yu & Cho (2004) [10]	Static	Neural Network	21	0	3.69
Gunetti & Picardi (2005) [12]	Static	Neural Network	205	0.005	5
Clarke & Furnell (2007) [8]	Static	Neural Network	32	5 (Equal Error Rate)	
Lee and Cho (2007) [14]	Static	Neural Network	21	0.43 (Average Integrated Errors)	
Pin shen The et al (2008) [27]	Static	Statistical	50	6.36 (Equal Error Rate)	

V. REVIEW OF APPROACHES IN KEYSTROKE ANALYSIS

A lot many numbers of studies [6], [8], [9], [10], [11], [13] have been performed in the area of keystroke analysis since its origin. There are two main keystroke analysis approaches for the purposes of identity authentication. They are statistical techniques and neural networks techniques. Some are the combinations of both the approaches. The basic idea of the statistical approach is to compare a reference set of typing characteristics of a certain user with a test set of typing characteristics of the same user or test set of a hacker. The distance between these two sets (reference and test) should be below a certain threshold or else the user is recognized as a hacker. Neural Networks process first builds a prediction model from historical data and then uses this model to predict the outcome of a new trial. Even though the studies tend to vary in approach from what keystroke information they utilize to the pattern classification techniques they used. All the attempts are made to solve the problem of providing a robust and inexpensive verification mechanism.

VI. REVIEW OF KEYSTROKE DYNAMICS SECURITY

Until now, very little research has been conducted to analyze keystroke dynamics security [12]. The application of keystroke dynamics to computer security is relatively new and not widely used in practice. Researches on real cases of breaking keystroke dynamics verification system do not exist. 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.

A) Shoulder Surfing- A simple way to find a user's password is to watch them during verification. This is called shoulder surfing. Regardless of if keystroke dynamics are used in the verification or classification type, shoulder surfing is no threat for the verification system. Password is not used in the classification case and therefore the password can't be stolen. Only the keystroke pattern is important and significant. In case of verification, an attacker may be able to find the password by shoulder surfing. However, keystroke dynamics for verification is a two-factor verification mechanism. The keystroke pattern still has to match with the stored profile.

B) Spyware – Spyware is the software that records information about users, usually without their knowledge. It is probably the best and easiest way to break keystroke dynamic-based verification systems. If a

user accidentally installs a Trojan which records all of the user's typing, keystroke latencies and keystroke intervals 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.

C) Social Engineering- Social engineering is the practice of finding confidential information by manipulation of legitimate users. 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 these techniques the social engineers take advantage of the natural tendency of a person to trust his or her word before 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 classification 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 to give away his keystroke pattern. The attacker might portrait as 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.

D) 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.

E) Brute Force- In this attack an intruder tries all possible combinations of cracking a password. The more complex password is more secure 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 verification 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 verification mechanism, that is password and keystroke, it is almost impossible to overpower the security system.

F) Dictionary Attack -A dictionary attack [4] is a technique for defeating verification mechanism by trying to determine its pass phrase by searching a large number of possibilities. In contradiction of a brute force attack where all possibilities are searched exhaustively. Dictionary attack only tries possibilities that are most likely to succeed which are typically derived from a list of words in a dictionary. As with brute force searches, it is impractical to carry out dictionary attacks against keystroke dynamic verification 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. Achieve 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.

VII. CHALLENGES

Keystroke dynamics is a behavioral pattern exhibited by a person while typing on a keyboard [6]. User verification through keystroke dynamics is appealing for many reasons such as: (i) it is not intrusive, and (ii) it is relatively inexpensive to implement, since the only hardware required is the computer [10]. Unlike other physiological biometrics such as fingerprints, retinas and facial features these remain fairly constant over long periods of time where as typing patterns can be variable. 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, the hands of a person can also get exhausted or clammy after extended periods of typing. This often results in major pattern differences over the period of time. The another significant problem is that typing patterns vary based on the type of the keyboard being used, the keyboard layout, whether the person is sitting or standing and the posture of person etc. The fact is that the distributed nature of keyboard biometrics also means that additional inconsistencies may be introduced into typing pattern data.

VIII. CONCLUSION

The potential of biometric technologies is promising. The use of biometric devices and applications continuously growing all over the world .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 research into biometric error testing

that is false rejection rate and false acceptance rate has been of keen interest to biometric developers. Keyboard Dynamics, being one of the cheapest forms of biometric and 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 other new ideas.

REFERENCES

1. Mrs. D. Shanmugapriya, Dr. G. Padmavathi, "A Survey of Biometric keystroke Dynamics: Approaches, Security and Challenges", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 5, No. 1, 2009.
2. Salil P. Banerjee, Damon L. Woodard, "Biometric Authentication and Identification using Keystroke Dynamics: A Survey", Journal of Pattern Recognition Research 7 (2012) 116-139 July 10, 2012.
3. FabianMonrose, Aviel D. Rubin, "Keystroke dynamics as a biometric for authentication", Future Generation Computer Systems 16 (2000)351–359 3 March, 1999.
4. N. Harun, W. L. Woo and S.S. Dlay, "Performance of Keystroke Biometrics Authentication System Using Artificial Neural Network (ANN) and Distance Classifier Method", International Conference on Computer and Communication Engineering, 11-13 May 2010, Kuala Lumpur, Malaysia, 2010 IEEE.
5. 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.
6. Monrose, F., Rubin, A., "Authentication via Keystroke Dynamics", Proceedings of the 4th ACMConference on Computer and Communications Security, p 48-56, April 1997.
7. 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.
8. Bergando et al, "User Authentication through keystroke Dynamics", ACM transaction on Information System Security" Vol.No. 5, pg 367-397, Nov 2002.
9. Enzhe Yu, Sungzoon Cho, "Keystroke dynamics identity verification and its problems and practical solutions", Computers & Security, 2004.
10. Gunetti and Picardi, " Keystroke analysis of free text", ACM Transactions on Information and System Security, volume 8, pages 312–347, 2005.
11. S Bleha and M S Obaidat,"Computer user verification using the perceptron," IEEE Trans. on Systems, Man, and Cybernetics, vol. 23,no. 3, pp. 900–902, May 1993
12. Benny Pinkas ,"Securing Passwords Against Dictionary Attacks", CCS'02, 18–22,November 2007.
13. Cho et al , "Web based keystroke dynamics identity verification using neural network", Journal of organizational computing and electronic commerce, Vol. 10, No. 4, 295-307, 2000.
14. Guven, A. and I. Sogukpinar, "Understanding users' keystroke patterns for computer access security", Computers & Security, 22,695–706, 2003.