



Analysis of Time Based Remote User Authentication Procedure

Sachin Raturi
Department of CSE,
Uttarakhand Technical University
Uttarakhand, India

Renu Bahuguna
Department of CSE,
Uttarakhand Technical University
Uttarakhand, India

Shashank Lingwal
Scientist/Engineer-‘SC’,
Uttarakhand Space Application Centre
Uttarakhand, India

Abstract: Nowadays Password itself should not be the only security barrier for the intruders for any type of authentication system. So the concept of 3D securities, one time password, Biometrics etc. came into the scene. In this abstract we are proposing and testing another barrier to provide more secure and improved authentication system which can work effectively if the password is even stolen or revealed. In this procedure unique typing style are tested which may vary or depends on the psychological state of the particular. In the initial stage of our work we are not taking overall typing style as a feature sample for the password, but still the time can be taken as a perimeter while setting up a password. Here we are considering time duration between hitting of password keys. So depending on the requirement of individual user this time gapping between keys can be recorded and considered as a feature for user authentication. While setting password by two individuals, our system set the password with time delay provided by the user. For finding out the accuracy limit we tried it for 10 times so that the accuracy limit can be calculated for each standalone or remote user. If total number of characters in any password are n then recorded number of delay are $(n-1)$ and calculated number of accuracy limit are $(n-1)$. Using this mechanism more than 1 security level can be created with number of interruptions and accurateness limits contingent on our area of curiosity for security. The delay is decided by the users and the accuracy limit was calculated by the system or can be decided by the user. The Accuracy limit is calculated by using Analysis of individual user dataset by Descriptive statistics classification mechanism in first stage. Which provides two different type of security barriers for the intruders and for higher security level higher level of time delay and higher level of accuracy limit can be configured. Higher number of characters in the password string will provide various levels of time delay. This system is purely separated with other authentication schemes and is not affecting any of the previously introduced schemes so can be integrated in any kind of digital user authentication schemes.

Keywords: Authentication; security; key pressing dynamics; user authentication; biometric; typing psychology.

I. AUTHENTICATION

Authentication is the procedure of influential whether somebody is the one who it is declared to be or not.[1] Authentication is categorized into four main types:

A. What user knows (Knowledge based?)

This type depends on something that the user knows, such as passwords, PIN codes, OTP and security question. It is the most commonly used method. The unassuming lucidity here, if you recognize the surreptitious watchword for an account, then you must be the proprietor of that account .

The compensations of this type are: there is no supplementary hardware and all the desirable is a database which saves the PINs or the hash value of the secret code. The problems associated with this type of authentication are: the password can be forgotten, stolen, or guessed.[2, 3]

B. What user has (smart card or credit card?)

This category be subject to on something the user possess, such as smart cards, mobile phone and latest electronic gadgets. It is used in automated teller machine (ATM). The lucidity here is if you have the smart card with you, you must be the proprietor of the account.[1, 3]The problems of this type: the card may be misplaced, whipped, or replicated by someone else.

C. What user is (Biometric based?)

This type depends on the human body features, such as finger print, iris, retina and hand geometry, finger vein, DNA based, palm vein. It is used in some banks to identify the users. This requires that the user can have specific humanoid characteristic that can be skimmed and digitally recognized.

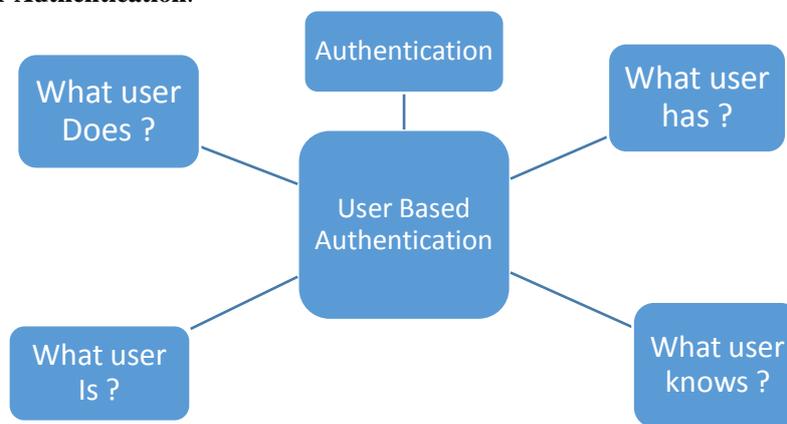
The benefit of this category of scheme is that biometrics could not be whipped neither mislaid. The problem/demerit is that this authentication system needs special tools and no body parts harm to do the scanning of the biometrics. Also, biometric substantiation is not appropriate in all circumstances, especially for remote authentication, distributed system authentication.[4, 5] Also, we cannot provide the machine which recites the biometric figures in all circumstances that

need substantiation. Moreover, not all biometric authentication techniques are acceptable by all people. [14] In addition to that, biometric substantiation procedures require precise environmentssuch as no vein blockage, ciliary muscles shrinkage in eyes and many otherwhich are not possible all the time.

D. What user does (Behavioral Based?)

This type depends on the user behavior, such as typing style, finger movement pattern and tapping pattern. Typing style, or as it is termed as keystroke subtleties, sometimes measured as the best behavioral based authentication system. It is the easiest and cheapest way, because no hardware is being needed, just the keyboard of any type.

Graphical way of User Authentication:



A review of comparison over security properties and computational cost of proposed scheme. Table [10] describes comparison of security properties.

Comparison of Security properties						
	Ali A. Yassin	Das et al.	Liao et al.	Wang et al.	Yoon and Yoo	Khan et al.
C1	Yes	Yes	Yes	No	Yes	Yes
C2	Yes	Yes	Yes	No	Yes	No
C3	Yes	No	Yes	No	Yes	Yes
C4	Yes	No	No	No	No	No
C5	Yes	No	Yes	Yes	Yes	Yes
C6	Yes	No	Yes	No	Yes	Yes

C1: Freely chosen password; C2: User anonymity; C3: Secure password change; C4: session key agreement; C5: Mutual authentication, C6: No password reveal.

II. EXTENDED AUTHENTICATION

Extended authentication is now taking the lead in this field. Password is not only one way to authenticate users remotely, especially when linking to private records, financial transactions systems or even communal networks.

Password authentication agonizes from many disadvantages and faults due to its nature. Since many people tend to use very simple and easy to reminiscePINs, they are frequentlyconnected to themselves and can be predicted easily. Moreover, people use the same passwords for many applications and websites.[6, 7] Some of these websites may transfer the password in an unencrypted manner which hints to be easily snuffled and reinstated. Another problem with passwords is typing the password very close to other person (Shoulder Surfing), [3, 7] some passwords characters are revealed.

Therefore, there is a prerequisite for additional procedure to be added to password substantiation. “What you have” [11] and “what you are” [12] are not valid over the internet. Then stirring to “what you do” [13] factor to be added to the password will reinforce the password substantiation mechanism.

Typing behavior is considered to be different for each user; different people have a tendency to have different keying behaviors. Therefore, counting the keying behavior in substantiation will convert password authentication more secure. The hacker is required to gain the user typing behavior now in addition to the password itself.

III. KEYPRESSING BASED AUTHENTICATION BASIC FEATURES

This survey paper focuses on the behavioral authentication and focuses on keystroke authentication. In order to collect data, most of the studies use one of two ways, randomized-based or continuous-based. Randomized-based mean fixed text, so the user has to enter the same text several times. Continuous-based or free-text mode, the data can be collected from any typed text, where the user may be required to type length based text, and features get collected.

There are several topographies which can be perceived when the handlers press keys on keyboards. Basic keystroke features are:-

- Duration or Hold (H): It is the time recess between a key is pressed and released (by considering individual keys) . For example, the time between pressing the letter 'x' and releasing it.[5, 7]
- Up-Down time (UD): It is the time interval between releasing a key and pressing the next key (by considering 2 keys).[4, 7]
- Down-Down (DD): It is the latencies between two successive key down presses (time duration between pressing 1st key and 2nd key). It is considered as the major feature data represented in keystroke dynamics domain . For example, the time from pressing "a" until the time of pressing "b", which includes the pressing time of "a".[1, 7]
- Up-Up (UU): It is the time between key-up of the first key and key-up of the second key; it is equal to UD + H of the second key.[3, 7]
- Down-Up (DU): It is time between key-down of the first key and key-up of the second key; it is equal to DD + H of the second key.[2, 3, 7]
- Pressing time: It is the time while the key is held down.[6-8]
- Releasing time: It is the time while the key is released.[7, 9]
- Overall speed: Variations of speed moving between specific keys. [1, 7, 8]
- Frequency of errors: How much some specific error repeats.
- Pressure: Used when hitting keys while typing (used only for keyboard in touch screens).[2, 3, 7]
- Finger Placement: Where the finger is placed or even the angel of the finger when pressing the key.
- Finger choice: Which finger is used on the key of the keyboard?
- Capital letters and special characters. This happens when the user prints any character followed by capital letter or special character which requires pressing on 'shift'; these in many cases require longer time than two consecutive small letters.
- Distance between letters. For example the distance between 'a' and 's' is larger than the distance between 'a' and 'p' on the keyboard which may require more printing time.

IV. PERFORMANCE CALCULATION

Performance of such keystroke analysis is typically measured in terms of various error rates, namely False Match Rate (FMR), False Non-Match Rate (FNMR) and Crossover Error Rate (CER).

A. False match rate (FMR):

The probability that the system erroneously contests the input arrangement to a non-matching prototype in the database. It measures the percent of invalid inputs that are imperfectly recognized. In case of resemblance scale, if the person is an imposter in reality, but the corresponding score is sophisticated than the brink, then he is preserved as genuine. This increases the FMR, which thus also depends upon the threshold value.

In statistics this type of errors is referred to as a Type I error.

B. False non-match rate (FNMR):

The possibility that the scheme miscarries to detect a match between the input pattern and a matching prototype in the databank. It processes the percent of legal contributions that are incorrectly rejected, which is in figures is devoted to as a Type II error.

Both error rates should ideally be 0%. From a security point of view, type II errors should be diminished, that is no fortuitous for an unauthorized user to login.[2, 3, 6] However, type I errors should also be intermittent because valid users get annoyed if the system rejects them erroneously.

Many performance results were reported for typing behavior authentication. For example, in 2014 the authors [1, 3, 4, 7, 9] of have used statistical model and static text on mobile devices and got (0.92%) FAR, and (1%) FRR with 315 users.

C. Crossover error rate (CER):

The rate at which mutually recognition and denunciation errors are equal. The value of the EER can be effortlessly acquired from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves.[3, 7] In general, the device with the lowest EER is the most accurate.

Author in reported (2%) EER with 58 users for their work, using dynamic text and with statistical model, while authors in reported (12.82%) EER with 63 users, using static text with ANN model.[7]

V. TYPING BEHAVIOR SECURITY BARRIER

The typing behavior authentication; as most biometric techniques has two phases:

- 1) The enrolment, where reference features are stored to compare with them at the actual authentication phase.
- 2) Actual authentication where a user wants to access a system.

Both phases are necessary for typing behavior authentication. In order to analyze the collected data, there are two main ways, statistical model and learning model. Statistical model compare reference typing characteristic with user typing characteristics.[3, 7, 10] However, learning model uses learning algorithms such as ANN and Genetic algorithms to learn and modify the user identity each time. A third approach is the hybrid which uses both statistical and learning models.[3, 4, 7]

First typing behavior authentication in desktop field have evolved between 1985 and 1990. Where studies showed a good fault resistance and they were improved over years.[12] With the usage of mobile devices many researchers conducted

many experiments on personal mobile digital devices, personal computer with their classical keyboards, laptops with special keyboards embedded in, and handheld devices with their special keyboards screens.[2, 3, 7]

The basic idea of typing behavior authentication approach is to compare a reference set of keying physiognomies of a certain user with a test set of typing characteristics of the same user or a test set of a hacker. The distance amongst these two groups (allusion and assessment) should be underneath a certain threshold or else the user is renowned as a hacker.

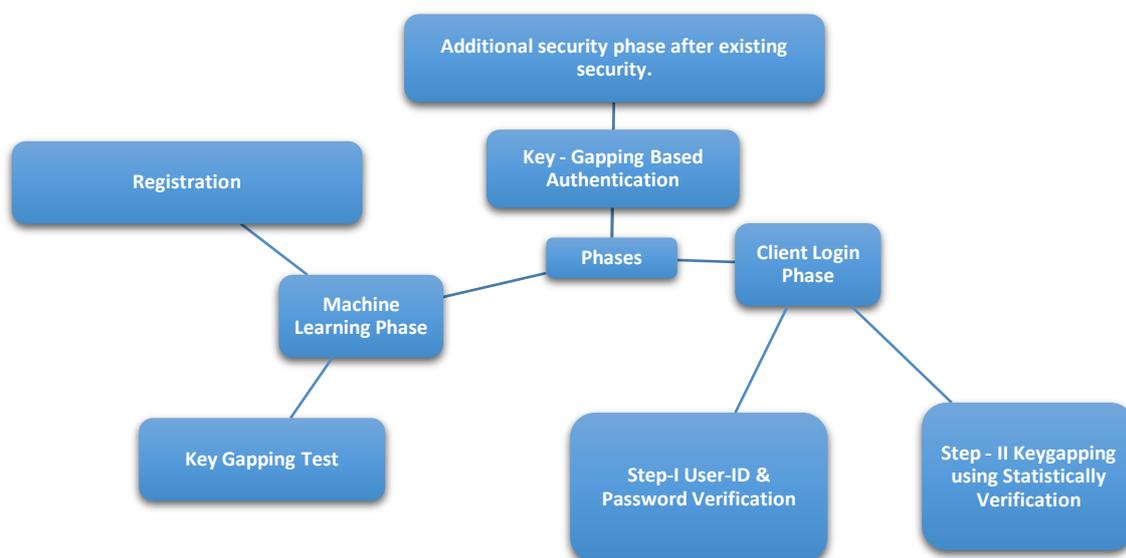
VI. FUTURE WORK DIRECTIONS

The latest typing behavior authentication research is moving towards different main paths which can be summarized as follow:

In the present study user authentication schemes has been taken as the core technology which provides secure and efficient remote user authentication. Smart card is a major constituent of this core technology. The main objectives of present study are-

- To find out security issues in existing models by analyzing traditional and modern user authentication models and schemes.
- To propose a secure and efficient remote user authentication algorithm or scheme with an aim to suggest solution for distributed networks.
- Investigates various issues involved in designing a novel model/algorithm/scheme of remote user authentication for cloud technology with an aim to suggest solutions in the form of many measures and management standards.
- Analyzes issues involved in user authentication for Smart phone devices and gadgets.

Graph for Future Work Directions



1-Secure HASH Machine Learn Phase

2-Statistically Analyzed One parameter with highly mathematized form

Most research papers were focusing on static text typing behavior authentication which seems to be stored without encryption techniques. These days, with the widespread use of ATM Card and the problems of losing them, there is more need to go towards dynamic authentication. In dynamic authentication, if somebody logged in to an ATM Machine, and then he/she lost the CARD, dynamic authentication can detect that the current user (the one who found it) is not the owner of that particular card because there is a difference in typing behavior between the two users. This behavior can only be discovered in dynamic keystroke based authentication.

VII. CONCLUSION

Password authentication is the most commonly used authentication method for local access, network access, and internet access. However, password authentication suffers from many drawbacks due to password nature. Therefore, some techniques are required to strengthen password. Above survey basically focused on typing behavior authentication techniques (also called keystroke authentication).

It is to be reviewed from above section that each and every method having their individual problem in fact using behavioral based authentication also need some correction which should be comparatively that must statistically analyzed two or more than two times with one parameter only not to multiple parameter and checked that the False Accept Rate (FAR) and False Rejection Rate (FRR) should be 0%.

REFERENCES

- [1] Premchand, P. and A. Govardhan, A smart card based remote user authentication scheme. Journal of Digital Information Management, 2008. 6(3): p. 256-261.

- [2] Nahin, A.F.M.N.H., et al., Identifying emotion by keystroke dynamics and text pattern analysis. Behaviour & Information Technology, 2014. 33(9): p. 987-996.
- [3] Ngugi, B., P. Tarasewich, and M. Recce, Typing Biometric Keypads: Combining Keystroke Time and Pressure Features to Improve Authentication. Journal of Organizational & End User Computing, 2012. 24(1): p. 42-63.
- [4] Ramzi Saifan, A.S., Dema Zaidan, Andraws Swidan, A_Survey_of_behavioral_authentication_us. 2016.
- [5] Salil P. Banerjee, D.L.W., Biometric Authentication and Identification using Keystroke. 2012.
- [6] Jayasree SAHA1, R.C., AN APPROACH TO CLASSIFY KEYSTROKE. 2014.
- [7] Zahid1, S., et al., Keystroke-based User Identification on Smart Phones. 2014.
- [8] Kotani, K. and K. Horii, Evaluation on a keystroke authentication system by keying force incorporated with temporal characteristics of keystroke dynamics. Behaviour & Information Technology, 2005. 24(4): p. 289-302.
- [9] Ilonen, J., Keystroke dynamics. 2011.
- [10] Misbahuddin, M., P. Premchand, and A. Govardhan, A smart card based remote user authentication scheme. Journal of Digital Information Management, 2008. 6(3): p. 256-261.
- [11] Hwang, M.-S., Li, L.-H.: A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics 46, 28–30 (2000)
- [12] Sun, H.-M.: An efficient remote use authentication scheme using smart cards. IEEE Transactionson on Consumer Electronics 46, 958–961 (2000)
- [13] Fan, C., Chan, Y., Zhang, Z.: Robust remote authentication scheme with smart cards. Computers and Security 24(8), 619–628 (2005)
- [14] Das, M.L., Saxena, A., Gulati, V.P.: A dynamic ID-based remote user authentication scheme. IEEE Transactions on Consumer Electronics 50(2), 629–631 (2004)