International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

Online Banking System using Template Based & Keystroke Dynamics Passwords

Hemant Nagpure, Vinayak Waikar, Arvind Khandelwal, Rupali Shishupal
Department of Computer Engineering
Sinhgad Institute of Technology (SIT)
Lonavala
University of Pune, India

***Abstract*— In this age of internet, as every system is interconnected the importance of information security is highly noticeable. Considering the millions of transactions happening every day and the confidential user data is being passed over to the system, the risk of harmful activities by the unintended user increases. To overcome all this threats more reliable, secure and hardware independent ways are required to authenticate the online systems. In our paper we have given the authentication methodology for the online banking system based on template based password and keystroke dynamics. Templates in addition to password having the benefit of one-time password can be as simple as week day or parity of the day. Keystroke dynamics to extract detailed timing information of users typing pattern is implemented.**

Keywords*— *Internet Banking, Keystroke Dynamics, Online Banking, Security in e-banking, Template Based Passwords.

I. INTRODUCTION

Online Banking is a web based platform to the user to access banking information and helps to perform transactions securely. A customer has to register with the bank first for the online banking facility to initiate. Later it has to authenticate every time whenever he/she want to login or perform transactions. The main context comes here is of the authentication which should be more secure, efficient and reliable. Only the user and the bank should know the information shared between them and no third party should be given access to the system by any means.

In order to be more secured many organizations have set up additional security steps for access, but there is no consistency to the approach adopted. There are many examples in the history about online system's security breach. Like the incident of spring 2012 in Iran, the disclosure of PIN of about three million debit cards, was a glimpse of the importance of a dynamic authentication method [2]. Internet has now become the part of people's day to day activities with the number of alternatives to access fast internet unlike the past. Thus with all this technological advancements there is a major need evokes about the information security and users integrity. When it comes to online banking system thousands of transactions are done by the users within the fraction of second. The authentication is done using a password verification method hence many hackers or intruders can get into the system [2].

Current authentication methods can be categorized as token-based, biometric or knowledge-based. Token-based techniques are widely used as in key cards, debit cards and smart cards. Many of them provide more security by using additional knowledge-based authentication, e.g. the PIN in debit cards. More authentication methods like Biometric authentication methods, such as fingerprint, iris-scan and face recognition, are yet to be publicly approved [2].

An authentication method must be resistant to the common attacks which are as follows [2].

1. Brute-force attacks: Attacker tries all the possible combinations to find the password in these attacks. Defense mechanism of them usually suggests such a domain for passwords; that testing all of them be not possible in a reasonable time, e.g. longer passwords.
2. Dictionary attacks: These attacks are based on different dictionaries of passwords, which are generated based on common words and phrases in users' passwords. Therefore, the attacker limits the testing to the combinations in those dictionaries.
3. Shoulder surfing attacks: The attacker looks over the shoulder of the user, and memorizes the combination.

To obtain the best authentication method for the online banking system, in our paper we have suggested two ways. In first place we will provide template based password for the login in the system. Template can be as simple as using week-days or as parity of the day. Each template can be added to the either end of passwords, therefore there would be numerous templates with two possible positions each; which provide security as well as simplicity. These templates can be changed by various parameters, e.g. time, and generating different passwords [2].

The other way is by using the keystroke dynamics to calculate the detailed timing information of the users typing behavior on the keyboard. Then storing this information in the database as a biometric template to authenticate the user every time he/she wants to perform the transaction in the

system. This is possible as some characteristics of keystrokes for each user are unique as a handwriting or signature. Therefore rather than using the traditional password authentication through this solution we can make sure whether the actual and intended user gains access to the system or not [1].

II. LITERATURE SURVEY

There is one method which meets the requirement of template based password i.e. one time password (OTP) which are generated by tokens and delivered to user. Its disadvantages are every time new password is generated and the user requires a device to receive that [2].

S. Benson Edwin Raj and A. Thomson Santhosh have proposed a biometric identification problem by focusing on extracting the behavioral features related to the user and using the features for computer security. Standardized mouse dynamics biometrics involves a signature that was based on selected mouse movement characteristics under different screen resolution and mouse pointer speed settings. Several experiments were conducted under different settings to form the mouse dynamics signature of the user. Earlier methods failed to give better results when performed under different screen resolution and mouse pointer speed. The proposed method standardizes the user signature irrespective of the setting making it more useful for security application. The mouse dynamics could be further standardized based on the mouse pointer speed. The combining standardized screen resolution and standardized mouse pointer speed would guarantee even better result [1].

It was concluded that the keystroke dynamics was a user friendly biometric authentication technique and already there are Keystroke Dynamics Based Human Authentication Systems using Genetic Algorithm available for online applications; web based emailing and other online services. It minimizes the impact on the user's privacy and was very simple to integrate. The keystroke pattern recognition technique could be used effectively as a safeguard to unauthorized access to computer resources and sensitive data [1].

Product	**Drawback**
Retinal Scanning[1]	Devices required (Camera) and are very intrusive. It has the stigma of consumer's thinking it is potentially harmful to the eye. Comparisons of template records can take upwards of 10 seconds, depending on the size of the database. Very expensive
Vasco Servers (Tokens)[1]	Very expensive and is difficult to understand
BehavioSec [1]	Not well-suited for detecting and preventing fraud. Problems with password-based identity verification

Table 1. Some existing solution and their drawback.

III. SYSTEM MODEL

We have divided our system into two phases. The first phase uses the template based password method whereas second phase uses keystroke dynamics.

Phase 1: Login using template based password

In this phase the user will be given a password with a template of his choice. For the first time login user has to enter the password which will be encrypted using the method where the password will be converted into bits. The odd and even bits are combined together in a sequence and sent to the server side as encrypted form. There the password will be decrypted and matched with the stored password in the database, and the corresponding template.

The template here could be anything like the date in solar, lunar or Julian calendar; or day of the week, or the parity of the date. We can add the template at either side of the password or whichever position we choose. Let the assumed password is “xyz”. Adding the template of parity of the day at the end position the password will become “xyz1” in odd days and “xyz0” in even days. If the day of week is selected as the template at first position, the password will be “2xyz” on Tuesdays and “5xyz” on Fridays respectively. These templates can be freely altered, similar to passwords, after authentication [2].

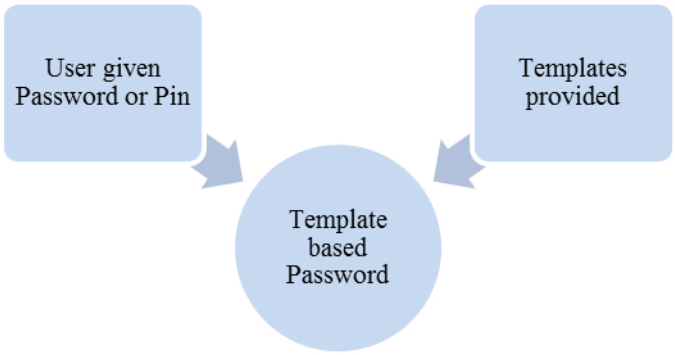

Fig. 1. Template based passwords

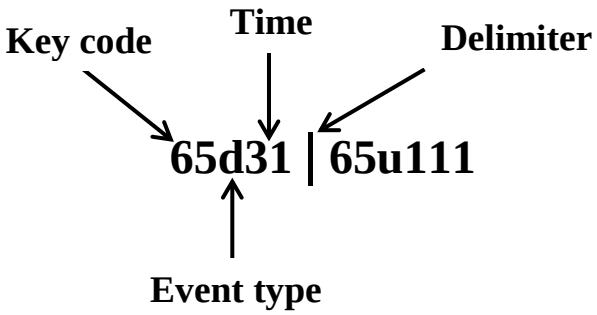

Fig. 2. A sample keystroke information for letter ***a*** [1]

Phase 2: Transaction using keystroke dynamics password

While performing transactions user will be prompted to create a password for the first time. To obtain the timing of users typing behavior, we developed a library using java script to track the keystroke timing information. The system extracts keystroke timing data at the client end, since it could obtain more accurate information. The system is tracked by handling "onkeydown" and "onkeyup" events in DOM (document object model). Html key code is used here to denote and keep a reference for each key. Next the time taken for each key press for a detailed string is added. By validating which event occurs accordingly, it is identifying if the user is adding d or u to denote whether it is a key press or a key release event [1].

KEY	HTML CODE
K	75
L	76
SHIFT	16
R	82
BACKSPACE	8

Table 2. Some key code references [1].

At this instance it is able to obtain elapsed time of dwell time from key-up time, because it takes the key-up time duration by subtracting from previous event time. This means the key down event. This dwell time is more crucial. Because, these key stroke times can be vary from device to device. Some key board layouts have more space in between keys and some are close enough to each. But, key down time, which is time between key down event and key up event, is independent from the layout of keyboard. Therefore the assumption as to give accurate result without dependency on the device [1].

To save the space in the database we store details as a whole string and we used pipe sign to delimit each key press event [1]. Then these details are matched every time user enters the password during transaction to proceed successfully.

We mainly developed two comparison algorithms to compare with the keystrokes consecutively when the user logins to the system. One is based on dwell time and the second is based on human frequency [1].

A. Dwell time based algorithm[1]

In this algorithm we are taking the elapsed time of Key down and key up.

X=t1 – t2----------(1)

Y=t3 – t4----------(2)

(1) / (2)

Z=X/Y

Where,

t1, t2: elapsed time of key down and key up at sign Up

X: dwell time of first attempt (sign up)

t3, t4: elapsed time of key down and key up at sign In

Y: dwell time of sign in

Z: deviation of X and Y

Confidence Level Check Information:

1.0 > Z > 0.9 = C: 95

1.2 > Z > 1.1 || 0.9> Z > 0.8 = C: 85

1.3 > Z > 1.2 || 0.8 >Z > 0.7 = C: 75

:

:

:

:

1.9 > Z > 1.8 || 0.2 > Z > 0.1= C: 15

Where,

C: confidence level of each key

We create a Boolean array of length similar to number of characters of particular string. If the C is lower than 50 then mark as false for particular element. Now we have two measurements. Mean of C and number of true elements of array has large value to validate. In here the confidence level 100> c > 70 concerned.

B. Frequency based algorithm[1]

This algorithm is developed based on human frequency. In here we check the deviation of frequency between same key on the keyboard when user presses it several times. In here also we used same keystroke timing information. Assume that user presses a particular character 2 times.

102d76 | 50u76----------(1)

105d76 | 60u76----------(2)

f1 = 102/50 = 2.04

f2 = 105/60 = 1.75

D = f1/f2

Where,

d = key down time

u = key up time

f1 = frequency of first key press

f2 = frequency of second key press

D = deviation of frequencies

In above calculation received f value around 0.857843. If the value approximate to 1 then it means those frequencies are close to each other. Considered the confidence level as 1 > d> 0.70. By retrieving the results of algorithm A and algorithm B we can obtain a better validation.

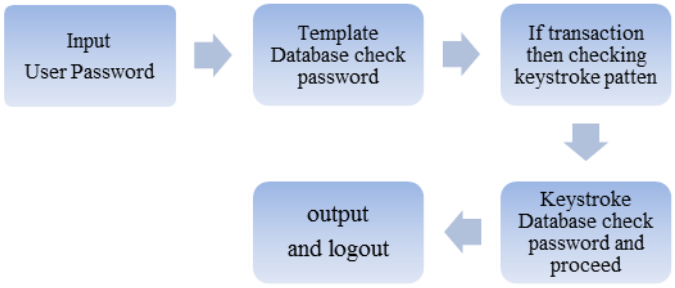

Fig. 3. Overall flow of the system

IV. CONCLUSION & FUTURE WORK

This method improves the security of traditional text-based passwords with a minor alteration. It provides security, simplicity, dynamicity and the ability to be used by the wide range of user. This method is not limited to use in banking service. Template-based passwords can supersede the traditional text-based password in different services. Our system with its algorithms is mainly focused on online banking users. But, these algorithms can be adapted to other online systems like e-mail services, social networks and even more critical environments like trading platforms. Since the logic behind this solution is simple and solid it can be adapted and implemented in most environments where security concern is a problem.

These algorithms can be adapted to other online systems like web based e-mail services, social networks and even more critical environments like trading platforms. It can be combined with the one-Time password to make more secure. The PIN in e-banking services, which is 4-digits long, can be altered so that one or two digits of it can be used for the template.

V. REFERENCES

1. N.M.Gunathilake, S.P.Koralagoda, M.G.jayasundara, "Enhancing the Security of Online Banking Systems via Keystroke Dynamics", The 8th International Conference on Computer Science & Education (ICCSE 2013) April 26-28, 2013. Colombo, Sri Lanka SuC2.5.
2. Mahdi Rahimi Ghazi Kalayeh and Hossain Kordestani, "Using Template-Based passwords for authentication in E-banking", 7th international conference 17-18 April 2013.
3. Xing Fang and Justin Zhan, Online Banking Authentication Using Mobile Phones, 2010 IEEE
4. Danish Jamil and Muhammad Numan Ali Khan, "Keystroke Pattern Recognition Preventing Online Fraud", International Journal of Engineering Science and Technology (IJEST), Vol. 3, No. 3, pp. 1953-1958, Mar2011.
5. O. Mangelschots, L. Meys, Vasco digipass, Orbit One International, 2008.
6. Weir, C. S., Douglas, G., Carruthers & Jack, M. (2009). User perceptions of security, convenience and usability for e - banking authentication tokens. Computers &Security, 28(1), 47–62.
7. Suo, X., Zhu, Y., & Owen, G. S. (2005). Graphical passwords: A survey. In Computer Security Applications Conference, 21st Annual.

8. [8] R. Chellappa, C.L. Wilson, S. Sirohey, Human and machine recognition of human face images: A survey, in: Proceeding of the IEEE, Vol. 83, 1995, pp. 705–741.

VI. APPENDIX

1. OTP-One Time Password
Create a unique password and sent to the user then valid user identifies this will not use again and again same password.
2. OMD-Object Modeling Design
3. UML-Unified Modeling Language
UML is used for visualizing, specifying requirements, gathering artifacts and documenting.
4. Keystroke-
When user pressed key of any device then there is Key press event occurs it also called as the keystroke.
5. GUI-Graphical User Interface
Users interact with GUI to avail the service of any application.