Journal of Basic and Applied Engineering Research
p-ISSN: 2350-0077; e-ISSN: 2350-0255; Volume 5, Issue 3; January-March, 2018, pp. 223-226

http://www.krishisanskriti.org/Publication.html

One-Pin Secure: User Authentication Scheme using Personal Device

M Hamza Zaki[1] and Muneeb H Khan[2]

[1, 2]Department of Computer Engineering Zakir Hussain College of Engineering and Technology
Aligarh Muslim University, Aligarh, India
E-mail: [1]hamza.zaki@zhcet.ac.in, [2]muneebhkhan@zhcet.ac.in

Abstract—*User Authentication is one of the main problems in present computing scenario. As machines become more powerful, the traditional authentication process becomes weaker. The problem of authentication becomes more serious in financial and banking system because banking transactions over internet are increasing day by day and these online banking systems require powerful authentication schemes. These systems are related to the basic asset of individual or organization which is money and lacunae in proper authentication will lead to big loss. At present the alphanumeric username/password combo is the most used authentication mechanism. However, this traditional scheme is not immune to wide range of attacks, like shoulder surfing, phishing, man – in – middle attack and many more. This paper proposes a robust authentication scheme which uses dynamic username and password like onetime password that eliminates static nature of login credentials and also reduces load on users of remembering long login credentials.*

Keywords: *Authentication, personal device, financial, shoulder surfing, phishing, one-time password.*

1. INTRODUCTION

Motivation behind this paper is to present an authentication system that eliminates most of the problems in traditional authentication scheme of username/password combo while keeping its simplicity. The username/password authentication scheme is simple in the sense that users just have to enter username and password to authenticate. There is no calculation, no recognition and no mapping that is no processing needed at user side. In comparison to this many graphical schemes exist which provide more security in comparison to alphanumerical passwords but they usually do not have the simplicity of authentication as describe above. Generally, these schemes force user to remember pattern or images and password is calculated from these patterns and this calculation of password increases authentication time. The scheme defined in [1] removes the static nature of username and password which is the main reason for different attacks as mentioned above. When username/password is dynamic, data breaching attacks become unsuccessful as there is no such data present to breach. Replay attack is impossible as username password is valid for limited period of time. Key logger attacks also become very difficult as its prime basis is static credentials of authentication. The paper is organized as follows: section 2 explains related authentication schemes, section 3 defines proposed work, section 4 analyses the scheme and section 5 concludes the paper.

2. RELATED WORK

Many authentication schemes are proposed that work on or one or more category of authentication as defined by Gorman[2]. Gorman classifies user authentication into three categories: first is knowledge-based (e.g. PIN), second is object-based (e.g. ATM card) and last one is ID-based (e.g.iris). Another fourth factor is given in [3] and is based on vouching. This concept defines the degree of authenticity rather than ayes ornodecision.

Google step 2verification technique[4]uses object-based category of authentication, since the user receives password on his mobile (object in possession of user) and provides a second level of security. The software generates random codes and sends them to the user's registered device in order to provide second level of verification in addition to the account password.

RSA Secur ID [5] is another popular system, which generate random code at fixed intervals (say every 30 or 60 seconds). Hardware token or software can be used to generate these codes. Hardware tokens need synchronization with the server for successful authentication.

Doodle based authentication scheme [6] is a type of graphical scheme and falls in the category of recall passwords. This scheme is somewhat similar to signature use for authentication in paper verification. Here users have to register their doodle/signature by drawing it digitally. The system stores user's strokes, direction of strokes and pressure exerted at different points and using all this information, feature vector is generated. Authentication is done based on the similarity of stored and input feature vector.

M I Awang et.al [7] proposed a pattern-based authentication scheme for minimizing shoulder surfing attacks. During

registration users have to choose any pattern and during login the user enters the password by following its pattern. Every time the grid is presented in different style by filling it either by characters, objects, numbers or images. This method minimizes shoulder surfing attack but does not eliminate it because the pattern user has chosen during registration is static and can be determined by the attacker if the user is constantly under monitoring.

A scheme based on predefined shapes is given in [8]. This verification scheme provides a set of indicators to the users (common shapes; e.g. squares, triangles and other polygons), following which the users can define their own pattern password.

Text based Pattern and Key (TPK) [9] password authentication scheme provides resistance to hidden camera and similar attacks and also increases the level of security. This scheme uses three layers of security to make passwords more secure. First layer consists of a pattern, second a key and last is a dummy variable. Users select pattern from 4x4 grid and choose a key of 9 digits and then select dummy variables that can be appended before or after the real password.

A pseudo dynamic password scheme [10], one-tip secure text-based password scheme [11] and a novel text-based user authentication scheme using captcha [12] discuss various challenge-response based techniques for user authentication.

Hyung Jun Shin et.al [13] proposed a secure pattern-based authentication scheme against shoulder surfing attack in smart devices. Two concentric circle structure is used. Both outer and inner circle can hold elements, for e.g. outer circle holds random numbers and inner circle holds random alphabets. The user enters his password by rotating these circles. Since only the user knows the right combination of outer and inner elements, this provides a dynamic password for authentication.

3. PROPOSED WORK

Proposed authentication scheme is different from other authentication scheme in the sense that it eliminates the need of remembering long login credentials and it is free from any graphical password and at the same time provides more secure authentication to its users. This scheme explained using two main phases, registration phase and authentication phase.

Block diagram of proposed registration phase is shown in fig. 1. The process explains how user register himself to this authentication scheme using his personal device. Personal device can be any electronic device that users can easily carry and that is able to perform cryptographic operations. Contemporary smart phone is the best example of such a device. Each device has a unique IMEI number and other details that are used to register the device for authentication.

3.1 Registration phase consist of following steps

In step 1 the user applies for online banking for his existing account in the bank. After confirming the validity of the user (to be a customer of the bank), the bank provides one-time reference number RFN which is step 2. In Step 3, the user installs the proposed bank app and completes registration using RFN provided by bank along with other details. Users also have to set 5 to 6-digit PIN in this step. Step 4 involves generation of cryptographic key pair by the app. This pair consists of public key p_1 and private key $d_1$which are saved after generation. The public key $p_1$is shared with registration server. In this step device also shares its unique IMEI number in order to uniquely identify and register the device. The last two steps involve transfer of message regarding success or failure of registration and display of this message to user. After successful registration process, user's device has its key pair, public key p_1, its private key d_1 and server's public key p_2.Serverhasits public key p_2, its private key $d_2$and user's public key p_1.

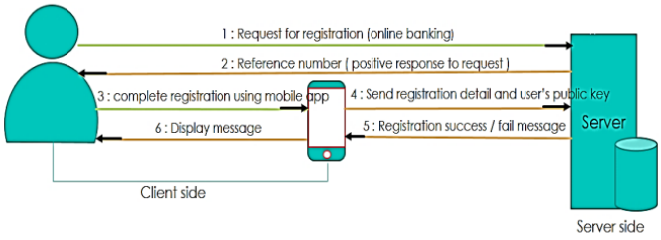

Fig. 1.Registration process

3.2 Login Phase:

During login first login credential (username and password) is generated. User's registered device communicate authenticating server to generate login credential. Step 1 to 5 showing this communication in fig. 2 and in step 6 user enter these generated credentials for login. At every login, username password is regenerated.

In step1 the user enters PIN which he sets during registration in order to generate a ticket. The generated ticket is shown in fig. 3. In step2 One Time Username (OTU)present in the ticket is displayed to the user. Ticket generated in step 1 is transformed and sent to the server in step3. The transformed ticket is shown in fig. 4. The ticket transformation steps are given below, where C represent cipher text.

I. C1 = signed (OTU) => encrypt OTU with user's private key 'd1'.

II. C2 = encrypted(OTU) => encrypt OTU using server public key 'p2'.

III. Device Id remains same.

IV. PIN is a user secret which the user sets during registration.

V. Mobile number is optional.

Server verifies user's ticket and sends him verification code/password in step 4. If ticket is verified, then server will perform following four sub steps.

I. Server decrypts C2 using its private key d_2 and gets decrypted text hereby named as "plaintext".

II. Server verifies signature C2 and let it produce decrypted text "plaintext2".

III. If "plaintext" = "plaintext2" then user is verified.

IV. If III is positive then C3 is sent to user's device. C3 is encrypted verification code using p_1.

In step5 user's device decrypt C3 with its private key d_1 and decrypted password is displayed to user in step6. Nonuser can use the OTU generated in step 2 and password in step 5 to login into his account, which is step7 and these credentials are valid up to the time whichever is earliest, 4 minutes or login.

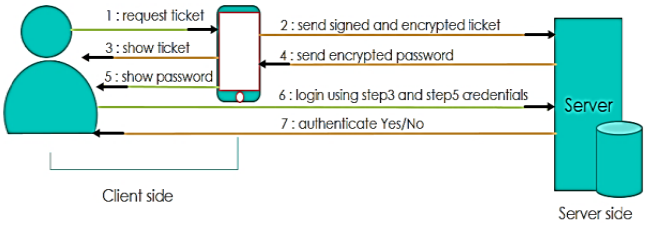

Fig. 2.Login phase

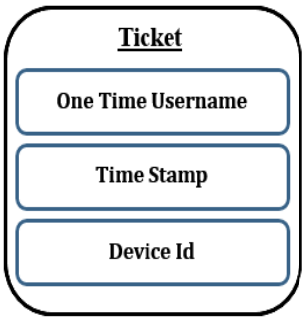

Fig. 3.Generated ticket

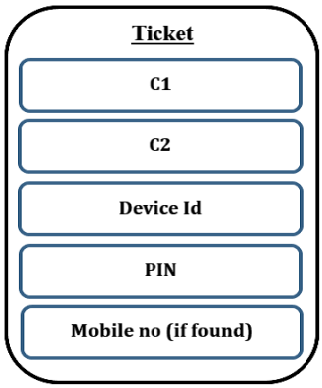

Fig. 4. Transformed ticket

4. RESULTS AND DISCUSSION

In this section security of the scheme is discussed along with its computational and communication overhead between client and server for authentication. Evaluation of this scheme was based on well-defined 25 different metrics of security, usability, and deploy ability, which is widely used to compare authentication scheme and is presented under the framework by Bonneau *et al*. [14].

4.1 Security Analysis

This scheme uses randomly generated username and password having the property of one-time pad. This property provides security against many attacks which rely on static login credentials and capture them in order to attack the user, for e.g. phishing, data breaching, key logger, shoulder surfing etc. This scheme also uses a PIN to resist any possible loss due to theft of the device. Security over network is provided by public key cryptography using the standard RSA algorithm. The password space of the proposed scheme is similar to alphanumeric passwords. Due to large password space and the one-time pad property, it is hard to do brute force attack. Table 1parameters are framework by Bonneau *et al*, shows the presence of different parameters of usability, deploy ability and security in various authentication schemes. The developed scheme (in green rectangle) is compared with four other schemes and it is found to perform better than all other schemes with respect to the parameters mentioned. Filled circle in a column representing a scheme indicates the presence of the benefit of the corresponding parameter in that scheme.

Category wise parameters / Schemes		Password	Google 2-Step [4]	MP-Auth [15]	PK Auth [9]	Developed
Usability	Memorywise-Effortless					•
	Scalable-for-Users					•
	Nothing-to-Carry	•		•	•	
	Physically-Effortless					•
	Easy-to-Learn	•	•	•		•
	Efficient-to-Use	•		•	•	•
	Infrequent-Errors				•	•
	Easy-Recovery-from-Loss	•		•	•	•
Deployability	Accessible	•		•		
	Negligible-Cost-per-User	•	•	•	•	
	Server-Compatible	•		•	•	•
	Browser-Compatible	•	•	•	•	•
	Mature	•	•			
	Non-Proprietary	•		•	•	•
Security	Resilient-to-Physical-Observation				•	•
	Resilient-to-Targeted-Impersonation		•	•	•	•
	Resilient-to-Throttled-Guessing		•		•	•
	Resilient-to-Unthrottled-Guessing		•		•	•
	Resilient-to-Internal-Observation					•
	Resilient-to-Leaks-from-Other-Verifiers		•			•
	Resilient-to-Phishing		•	•	•	•
	Resilient-to-Theft	•	•	•	•	•
	No-Trusted-Third-Party	•	•	•	•	•
	Requiring-Explicit-Consent	•	•	•	•	•
	Unlinkable				•	•

Table 1 shows the presence of different parameters of usability, deploy ability and security in various authentication schemes. Filled circle indicates the presence of the benefit of the corresponding parameter in a given scheme.

4.2 Performance Analysis

Performance in terms of number of bytes used by single user in order to authenticate himself from server is covered under communication overhead. The computational overhead includes total time taken in the process of authentication.

4.2.1 Communication overhead:

It is calculated from the size of ticket sent to server and verification code received by the client from server. Figure 4 ticket consists of 'C1' = 1024 bits + 'C2' = 1024 bits + 15-byte device Id + 5-byte PIN + 8-byte timestamp = 284 bytes. Server sends verification code/ password which is encrypted and its size is 128 bytes. So total communication overhead = 412 bytes as shown in Table2

Table 2: Communication overhead.

One user request		N user request
Communication overhead	412 bytes	(412 * N) bytes

4.2.2Computational Overhead:

There are two main computational operations: encryption or decryption and signature or verification, which are processes on both client and server side. RSA (1024 bit) keys are used for encryption/decryption. Table 3showstime taken in computational operations of both client and server side for single user. Total computation cost is 301 ms. Thus, authentication time is given as:

Authentication time = 301 ms + time taken in traditional authentication of username and password.

Table 3: Computation overhead of client and server side authentication processes.

Processes	Client-side process time (ms)	Server-side process time (ms)
Encryption	52	52
Decryption	45	52
Signature	50	Not done
Verification	Not done	50
Computation overhead	147	154

5. CONCLUSION

Evolution of e-commerce and e-banking systems has taken place at a rapid pace in the last few decades and growth of such systems has led to a huge increment in the number of usernames and pass words handled by individual users. Traditional authentication schemes have static credentials and because of this it suffers from large number of security issues. Users have a tremendous load of remembering large credentials and there fore start using same credentials for various accounts and systems. Attack on one account also endangers other accounts of the same user. The developed scheme is an authentication model that helps users to get rid of memorizing large usernames and passwords and at the same time is highly secure and efficient. Thus it can be very useful for financial systems. Moreover this scheme uses a pin to eliminate the problem of unauthorized authentication in case of device theft.

REFERENCES

[1] A. Alhothaily, Chunqiang Hu, A. Alrawais, T. Song, X. Cheng, and D. Chen, "A Secure and Practical Authentication Scheme Using Personal Devices" in open access journal of IEEE, Vol. 5, no. 10, pp 11677-11688, 2017.

[2] L. O'Gorman, ``Comparing passwords, tokens, and biometrics for user authentication, " *Proc.EEE*, vol. 91, no. 12, pp. 2021_2040, Dec. 2003.

[3] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, ``Fourth-factor authentication: Somebody you know, " in *Proc. 13th ACM Conf. Comput.Commun. Secur.*, 2006, pp. 168-178.

[4] *Google 2-Step Veri_cation*, accessed on Nov. 29, 2017. [Online]. Available: http://www.google.com/2step

[5] *RSA Securid*, accessed on Jan. 29, 2018. [Online]. Available: https://www.rsa.com/en-us/products/rsa-securid-suite

[6] Marcos Martinez-Diaz, Julian Fierrez, and Javier Galbally, "Graphical Password-Based User AuthenticationWith Free-Form Doodles, " in IEEE transactions on human-machine systems, 2015.

[7] M I Awang, M A Mohammad, R Mohaamed, An Ahmad, N A Rawi, " A Pattern-Based Password Authentication Scheme for Minimizing Shoulder Surfing Attack", International Journal on Advanced ScienceEngineering Information Technology, Vol.7(2017).

[8] J. Chen, D. Lopresti, and F. Monrose, "Toward resisting forgery attacks via pseudo-signatures, " in *Proc. 10th Int. Conf. Document Anal. Recog.*, 2009, pp. 51–55.

[9] M. Hamza Zaki, Adil Husain, M Sarosh Umar, Muneeb H Khan, ``Secure Pattern Key BasedPassword Authentication Scheme", in Proc. of *Int. Conf. onMultimedia, Signal Processing and Communication Technology*, Nov 2017

[10] Ramsha Fatima, Nadia Siddiqui, M. Sarosh Umar, Muneeb H Khan, " A novel text based user authentication scheme using pseudo-dynamic password", in Proc. of3rdInt. Conf. on Information and communication technology for competitive strategies, Dec 2017, Udaipur India.

[11] Zainab Zaheer, Aysha Khan , M. Sarosh Umar, Muneeb Hasan Khan, "One-tip Secure : Next-Gen of Text Based Password", in Proc. of 3rd Int. Conf. on Information and communication technology for competitive strategies, Dec 2017, Udaipur India.

[12] Atiya Usmani, Amrah Maryam, M.Sarosh Umar, Muneeb Hasan Khan, "New Text Based User Authentication Scheme using CAPTCHA", in Proc. of 3rd Int. Conf. on Information and communication technology for competitive strategies, Dec 2017, Udaipur India.

[13] Hyungjun Shin, Daeyoung Kim, Junbeom Hur, " Secure Pattern-Based Authentication against Shoulder Surfing Attack in Smart Devices", 2015 Seventh International conference on Ubiquitous and Future networks

[14] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, ``The quest to replace passwords: A framework for comparative evaluation of web authentication schemes, " in *Proc. IEEE Symp. Security Privacy (SP)*, May 2012, pp. 553-567

[15] M. Mannan and P. C. van Oorschot, ``Leveraging personal devices for stronger password authentication from untrusted computers, " *J. Comput. Secur.*, vol. 19, no. 4, pp. 703-750, 2011.