



Secure Web Authentication by Multifactor Password a New Approach

Shinde Swapnil K. Patil Yogesh N. Godase Avinash P.
Computer Engineering Department
Dr. Babsaheb Ambedkar Technological University, Lonere.
Tal-Mangaon, Dist- Raigad. Maharashtra.
INDIA

Abstract: Today's days the whole world is connected by web but facing the problem of trusted authentication. The main drawback in authentication is Password. The common authentication method which contains only the user name and the password has significant drawbacks. Users often use the password that is easy to guess if the password is not easy then it also difficult to remember, to overcome this drawback some researchers have suggested a picture password is another alternative to make secure authentication over web.

In this paper we had done the survey of various multifactor authentication techniques and suggested a new authentication method that uses multiple factors for making authentication (text, code, picture and sound). We are considering three steps to make authentication as knowledge base, Picture base, Personal authentication by using mobile phones. We think that our system will provide well secure authentication as compare to common authentication method. We resisted various security attacks at different steps of authentication. Our aim is to provide stronger authentication.

Keywords: Authentication, Multifactor, Picture Password, Security Attacks.

I. Introduction

The current situation where many passwords used in practice are either weak- and-memorable or secure-but difficult-to-remember, despite the need for secure and memorable passwords. The term Authentication describes the process of verifying the identity of a person or entity. It is the process of determining whether someone or something is, in fact, who or what it is declared to be. Authentication methodologies are numerous and range from simple to complex. The level of security provided varies based upon both the technique used and the manner in which it is deployed. The most prevalent form is probably the authentication with a user name and a password. Unfortunately it is also one of the most insecure methods. There is an unlimited range of variations of how a user can be authenticated to a web application. Some of the most popular ones are going to be described in the following.

Authentication methods can involve up to three factors:

1. **Knowledge:** What a user knows (i.e., a password or challenge question)
2. **Possession:** What a user has (i.e., a security token or mobile phone)
3. **Attribute:** What the user is (i.e. biometric characteristics like a fingerprint or the pattern of the eye)

Possession based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number.

1. Single Factor Authentication:-

Basic user name/password authentication for example is based on something you know. In single factor authentication user can use only one factor for authentication from above given factors. Usually user uses knowledge factor (i.e. Password or PIN). This case password may be textual or the graphical password or the PIN.

2. Multi Factor Authentication:-

In multi factor authentication user consist with more than one factors for security purpose the multifactor consist combination of what the user knows (i.e. PIN or password) and what the user has (i.e. smart card) and what the user is (i.e. biometric authentication).

Multifactor authentication also consist of more than once the same factor also means the user can use more than once any one of the above factor (i.e. what the user knows, what the user has, what the user is)

These methods have varying levels of security and impose different levels of inconvenience to the end user. An example is an ATM card. The card represents something you have, the PIN represents something you know, and hence it is a two factor authentication.

Strong authentication is also commonly referred to as two-factor authentication or multi-factor authentication. This alludes to the fact that there is more than one factor, or proof, needed in order for an authentication to be made. When only one factor is utilized to authenticate a user, it is considered to be a weak form of

authentication. Multi-factor authentication may include multiple types of the same authentication method (for example, two static passwords) but would not necessarily be considered strong authentication.

In this paper we had done the survey of various hybrid or multifactor authentication techniques and proposed our new scheme to make secure authentication.

The rest of the paper is organized as follows. Literature survey in Section II. Our proposed scheme III. Concluding remarks are given in section IV.

II. Literature Survey

In this survey we studied different hybrid authentication techniques and find some drawbacks in these techniques.

GP based systems for small mobile devices Khan [1] proposed a scheme for small mobile devices which takes drawing as input in authentication phase. The input is given by mouse or stylus according to the objects (pictures) selected by user priori in registration phase.

Gao [2] proposed and evaluated a new shoulder-surfing resistant scheme called Come from DAS and Story (CDS) which has a desirable usability for PDAs. It requires users to draw a curve across their password images (pass-images) orderly rather than click directly on them. This scheme adopts a similar drawing input method in DAS and inherits the association mnemonics in Story for sequence retrieval. It requires users to draw a curve across their password images (pass-images) orderly rather than click directly on them. The drawing method seems to be more compatible with people's writing habit, which may shorten the login time. The drawing input trick along with the complementary measures, such as erasing the drawing trace, displaying degraded images, and starting and ending with randomly designated images provide a good resistance to shoulder surfing.

Oorshot [3] proposed a hybrid authentication approach called Two-Step. In this scheme users continue to use text passwords as a first step but then must also enter a graphical password. In step one, a user is asked for her user name and text password. After supplying this, and independent of whether or not it is correct, in step two, the user is presented with an image portfolio. The user must correctly select all images (one or more) pre-registered for this account in each round of graphical password verification. Otherwise, account access is denied despite a valid text password. Using text passwords in step one preserves the existing user sign-in experience. If the user's text password or graphical password is correct, the image portfolios presented are those as defined during password creation. Otherwise, the image portfolios (including their layout dimensions) presented in first and a next round are random but respectively a deterministic function of the user name and text password string entered, and the images selected in the previous round.

RAYS' SCHEME [4] proposed a 3steps, step1 and 2 for registration and step 3 for authentication. In step 1 user need to enter textual username and password(password should belongs to Standard criteria) and 2nd step user need to choose the objects from the screen and assign them numbers from(1-9)and 3rd step of authentication user need to draw that objects in correct sequence as they entered in step2 on touch sensitive screen.

After survey we concluded some threats in these schemes and shown in following Table 1.

Attack	Khan Scheme	Gao Scheme	Oorschot Scheme	Ray Scheme
Brute Force Search Attack	✓			
Shoulder Surfing Attack	✓			✓
Man in middle			✓	
Spyware	✓	✓		✓
Social Engineering				

Table 1. Survey Result

III. Proposed scheme

I have proposed a Hybrid password Authentication scheme by considering combination of knowledge base, picture, sound and personal authentication through mobile phone.

Factor 1- in factor 1 we considering knowledge base plus personal authentication through the mobile phone. In this factor according to username one security question is send on your mobile phone as message and the user need to enter the answer of that question as password. The question is related to personal information of the user.

Why this?

Personal authentication is very secure authentication. Rather than sending one code on mobile and then verifying is create some problem as somebody stolen the mobile and got the one time secret code then he can easily enter in the system if he know your user id and password.

On the place of that we are sending a message as secret question rather than sending code. If somebody stolen that mobile but he can't easily answer that secret question. So it increases level of authentication. The question is wholly based on the secret information and only right user can answer that question.

Factor2- In this factor we are using a Recognition base Graphical password which is resistant to shoulder surfing attack and resistant spyware, screen scrapper as well as social engineering, difficult to guess and Dictionary attack.

We are extending here the authentication technique suggested by man et al. [5]. We are making some advancement in that to make it resistant to Man-In-Middle attack.

Man et al. given a unique number to every object on the screen and at the time of registration user select the images from the screen and remember the unique number associated with that image at the of authentication user need to enter that unique number associated with registered object. This system is resistant to shoulder surfing but vulnerable to man in middle attack. So we had made some changes.

Advancement- Rather than giving a unique number to every image on the screen and create old problem of remembrance. We are assigning a random number to image and numbers on that images are changes randomly from login to login and also changes the positions of the images on the screen. At the time of registration user enters the numbers shown on image as password but need to be concentrate only on images not on the number. Because we are creating purely image dependent system. The numbers entered by user get stored at back end in server. When user comes for login he sees a different numbers associated on images. He need to search out his registered images need not to worry about numbers. Enter numbers associated with those images.

Factor 3- In third factors we are using cued click recall based technique with the integration of sound signature. As this technique Is already suggested by Saurabh Singh [6] this technique suggest that user need click on more than one images rather than giving multiple click on single image so this technique is very difficult to guess and sound signature allows user to easily remember the password.

Why this? This technique is having more than one click but not on the single image. It having more than one click on number of images, so it have large password space, can't be easily guessed and includes with that a sound signature. Means after every click on image it generates sound. If click is correct then generates particular sound if not then generate random sound. Means this technique is strongly resistant to well known phishing attack.

The flow of scheme at the time of authentication –

1. In registration stage user needs feel all the details asked in the form. It collects all the details in server and generates the question based on the information filled on the form. The random question generator is used to generate random question and send over mobile phone through message.
2. In First step user need to enter the answer of the secret question as a password. So it get authenticate your mobile phone. If he answered wrong then authentication can't be performed onwards. User allowed going for second authentication step but not get authenticated at any step onwards and finally after last step get message Authentication failed. Due to this, he can't at which step he entered a wrong password.
3. In second step user needs to needs to enter recognition based graphical password by entering a random number on the image as he selected the image at registration but must be in the sequence. If user entered password correct then allows to enter third step and authentication in third step get activated and shows correct images for third step as he selected during registration. If user entered wrong password then allows entering in third step but authentication is deactivated. And user finally get message authentication failed.
4. In third step we are using clued click recall base authentication with the integration of sound signature. It generates sound after every click by the user. If it click correctly then generate the correct sound otherwise generate random sound.

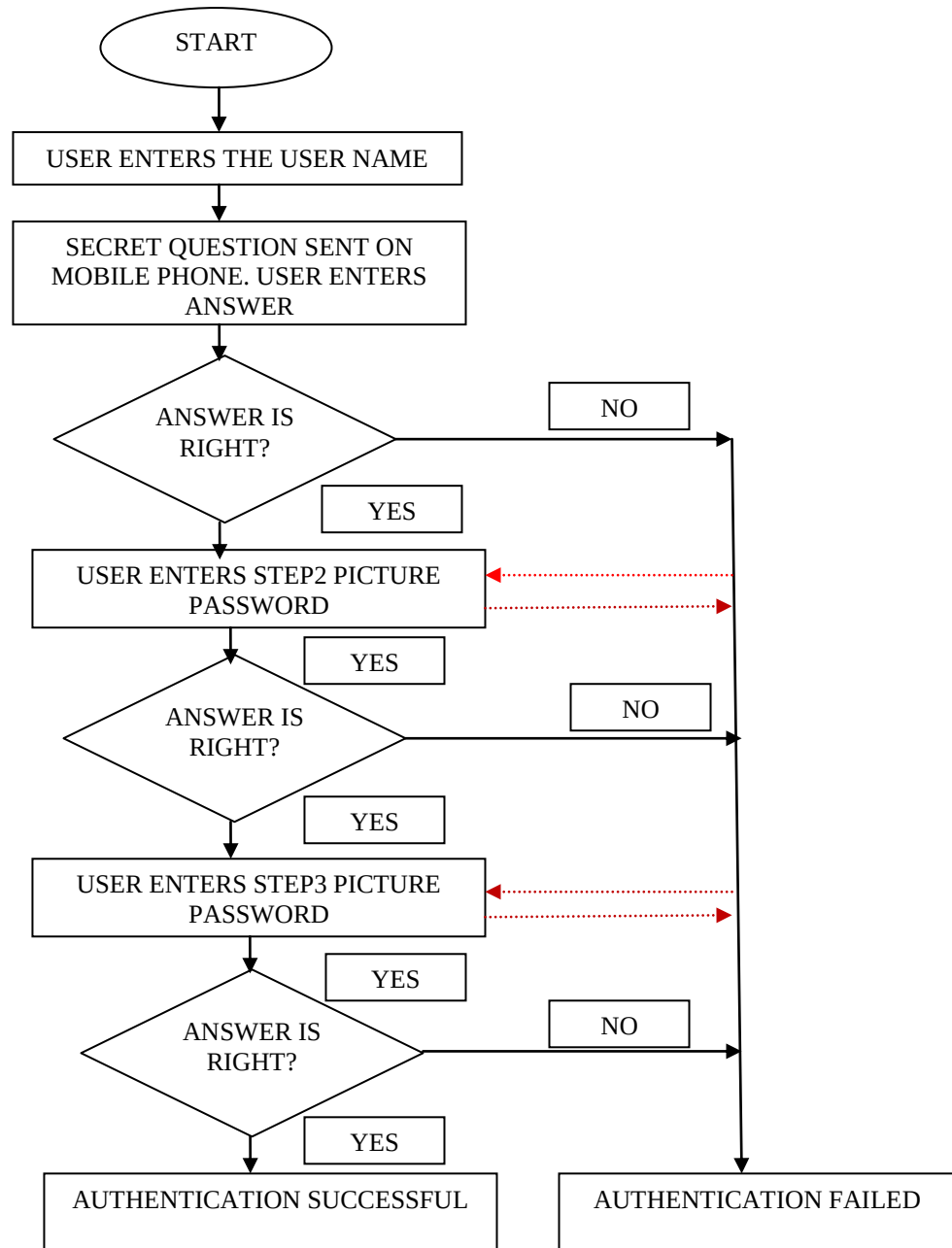


Fig1. Flow of Authentication System.

IV. Conclusion

In this paper we described our proposed scheme, flow of authentication system currently we are implementing this scheme for web server application to make secure authentication. This scheme is very easy to understand and use and we think so it replaces the currently available common authentication system.

This system is having drawback that it requires more time to make authentication. But it should be resistant to several security attacks such as shoulder surfing , man in middle, spyware, brute force, and strongly resistant to social engineering and phishing attacks. This scheme is having resistivity against different attacks at different levels user need to pass all these hurdles to get successfully authenticate.

V. References

- [1] Khan. W. Z., Aalsalem. A. Y., Xiang. Y. (2011), A graphical password based systems for mobile devices. *Internation Journal of Computer Science and Issues*, Vol. 8, Issue 5, No. 2, 145-154.
- [2] Gao, H., Guo, X., Chen, X., Wang, L., and Liu, X. (2008), YAGP: Yet another graphical password strategy, *Annual Computer Security Applications Conference*
- [3] Oorschot, P. C. V., Wan, T. (2009), TwoStep: An Authentication Method Combining Text and Graphical Passwords. *4th International Conference, MCETECH*
- [4] *International Journal of Computer Trends and Technology- volume3Issue2-*
- [5] . Man, D. Hong, and M. Mathews, "A shouldersurfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.
- [6] International Journal of Computer Applications (0975 – 8887) Volume 12– No.9, January 2011