Two Factor Authentication System using Intervened password and Color Pattern

Katta Shyam Prasad, Dr.Aruna Varanasi, Ummaneni Vinay Kumar

Abstract - Authentication is a key pillar for secure systems and enterprises are more and more aware that simple text passwords are not a strong form of authentication. A text password is inherently weak. Using text passwords for authentication, as it is commonly done, has quite a few security drawbacks: passwords can be guessed, forgotten, written down and stolen, eavesdropped or deliberately being told to other people. A better, more secure way of authentication is the so called "two-factor" or "strong authentication", instead of authenticating with a simple password. Strong authentication solutions using two identification factors require often an additional device, which could be inconvenient for the user and costly for the service providers. To overcome the difficulties we introduced a two-factor authentication which doesn't require any hardware device such as an authentication token or a hardware device to authenticate the user. The first factor is an Intervened text password more secure than a traditional text password and the second factor is a grid of Color Pattern.

Index Terms- Security, Authentication, Password, Color Pattern, Time gap, Two-factor, Intervened Password, Color Pattern, Encrypted, Decrypted

1. INTRODUCTION

The Two factor authentication system is an innovative technology used to solve the existing problems of the present one factor authentication which is a simple username and a password. In this system there are two factors or phases. The authentication of a user happens in two steps and by the user providing the system with two passwords. One password is the text password with certain time constraints set by the user during registration. The second password is the Color Pattern that will be generated by the user when he/she registers for the account. This system aimed towards the realization of a strong two factor authentication without using any hardware device to

- Provide with a cost effective and user friendly authentication.
- Avoids the use of a simple username and password system which is not secure anymore.
- Avoid the use of any hardware device as your authentication token.
- Ease to use any existing applications on web
- No additional use of hardware
- Easy to deploy

2. EXISTING SYSTEM

There are three universally recognized factors for authentication that exist today: what you know (e.g. passwords, PIN's), what you have (e.g. smart cards or tokens), and what you are (e.g. figure prints, face recognition, biometrics, etc.) —Two factor authentication is a mechanism which implements two of the below mentioned factors and is therefore considered stronger and more secure than the traditionally implemented one factor authentication system. There are several systems for dealing with two factor authentication.
Some of them are as follows:

2.1 Tokens

A token [1] is a device used to authorize the user with the services. A token may be software or hardware. Software tokens are used to identify the person electronically, i.e. it may be used as a password to access something. Hardware tokens are small hand held devices which carry the information which stores cryptographic keys, digital signatures or even bio-metric data by which we can send generated key number to a client system. Mostly all the hardware tokens have a display capability. The hardware tokens include a USB, digital pass etc.
Drawbacks:

- A token shall be carried all the time.

- Special software is required to read the token.
- Anyone can access the information that has the token i.e. in case of theft.

2.2 Biometrics

A biometric authentication [2] is the advanced form of authentication. A biometric authentication is nothing but it scans the user's characteristics such as finger print and eye retina and stores in the form of a string. When the user tries to authenticate it matches with the stored data and then gives access when a commonality is achieved and when the user has gained access he can enter the password to view the required information.

Drawbacks

- Biometric authentication is convenient only for limited applications, since the system becomes very slow for a large number of users.
- Finger prints can be taken on a small tape and can be provided for the hardware.
- Additional hardware is required to detect the fingerprints and eye retinas.

2.3 Mobile ID

Mobile Id [3] offers a strong two way authentication by authenticating the user to the service and service to the user. The mobile id works is such a way that the user is required to send the code generated by the application after which the Mobile id generates a code to identify the user with the service.

Drawbacks

- Mobile phones with 2.5 G and third generation only are supported.
- Software is to be installed into the mobile device.

2.4 One Time Password (OTP)

One time password [4] uses information sent in an SMS to the user as part of the login process. One scenario is where a user registers their information on a website. During this time the user is also asked to enter his or her telephone numbers. The next time the user logs into the website, they must enter their username and password; if they enter the correct information the user will be instantly called or sent a SMS text message with a unique, temporary PIN code. The user then enters this code into the website to prove their identity, and if the PIN code entered is correct, the user will be granted access to their account.

Drawbacks

- One time password (OTP) methods are also vulnerable to man-in-the-middle (MITM) attacks because the victim, unaware of the intruder, willingly enters the temporary pin to the website, unwittingly providing the intruder access to their account.

3. PROPOSED SYSTEM

In this system we are designing a more secure two-factor or dual-phase authentication. As the first factor the user has to authenticate by giving the Username and a text password. The second factor of authentication is the Color Pattern. The two-factor authentication that we have provided doesn't require any hardware device and is more secure compared to the other two-factor authentication systems.

During registration of the first phase the user has to fill in their details along with the Username and Intervened Password. We have added a special feature to the traditional Username and Password. For more secure authentication we have introduced a time gap between the characters or group of characters of the password as per the user's wish. The Password along with the time interval that the user gives gets registered in the database. For the user to estimate time gap a timer has been provided. The time gap should be minimum of 2 seconds. During login of the account the user has to give the Username and then the password with the same time intervals as given during registration or else the authentication fails. The time gap with a variation of +1 or -1 is accepted as a user may not be exact in giving the time interval.

During registration of the second phase we have introduced a 4*4 color pattern, the user can select a combination consisting minimum of 4 colors and maximum of 16 colors. The colors get rearranged every time the page is refreshed during confirmation of the pattern. This provides a more secure authentication as it prevents others to interpret the pattern based on the position of the colors. The pattern is encrypted and stored in the database to prevent any misuse by others. During login if the pattern matches with the one registered the user is authenticated.

In case the user forgets the password or pattern he/she has to validate themselves by answering the security questions or by giving the Email Id of the user. Once validated the password and pattern is sent to the user's mail id.

Algorithm for the proposed system:

Step1: Start

Step2: The user enters the Home page consisting of two fields- Username and Intervened Password. In case of an existing user go to step 6 else click on 'Register' button or if the user forgets the Password or color Pattern go to step 9.

Step3: In Registration page, user enters fields like Name, Username, Intervened Password, Confirm Password, Date of birth, Email id and phone number. All the details are stored directly in the database.

Step4: In Color Registration page, user selects a color pattern and in the next page confirms the pattern. The order of the colors changes each time the user logins and confirms the pattern. The registered pattern is encrypted and stored in the database.

Step5: In Security Registration page, the user has to answer two security questions, then page directs to Home page.

Step6: As the first-factor of authentication the existing user enters the Username and Intervened Password and clicks on 'Login' button.

Step7: As the second-factor of authentication the user selects the pattern as registered which ranges from 4 colors to 16 colors. In case the user entered a wrong pattern he/she can reselect the pattern by selecting the 'Reselect' button.

Step8: User profile opens after successful two-factor authentication.

Step9: In case the user forgets the Intervened password or Color pattern he/she clicks on 'Forgot Password'.

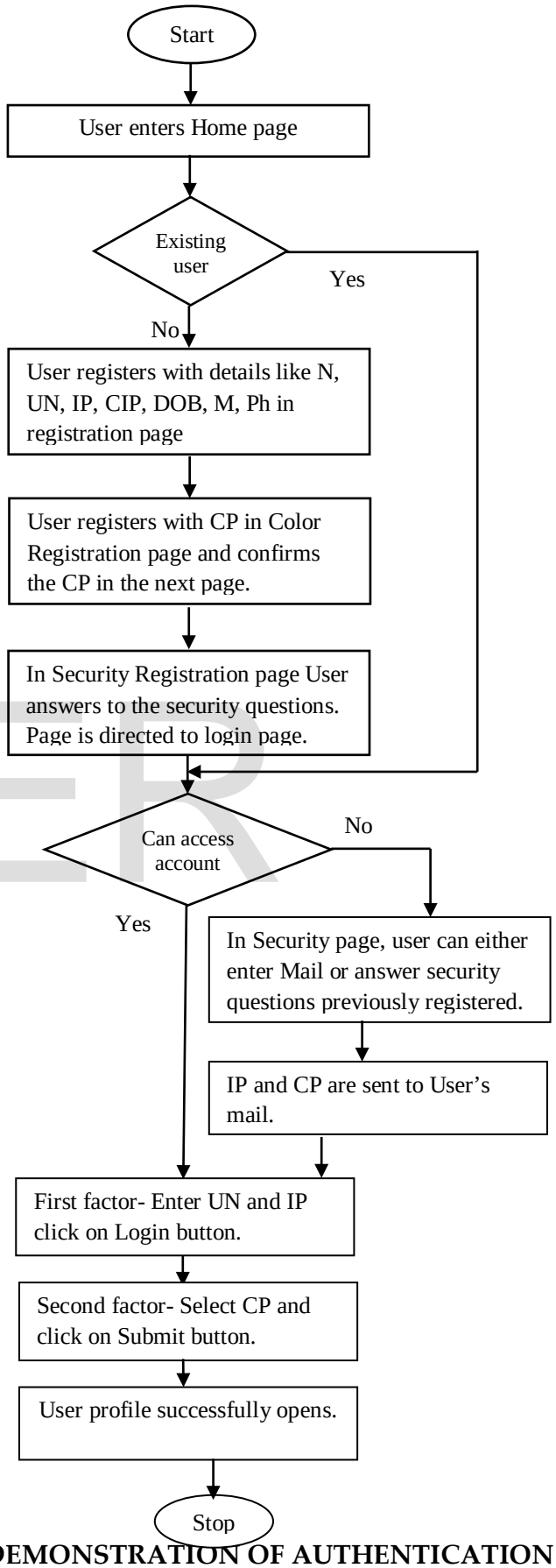
Step10: Security page opens wherein the user has two options either to enter his registered mail id or to answer the previously registered questions correctly. In either case of valid confirmation a mail containing Intervened Password and Pattern is sent to the user's mail id.

Step11: The user can successfully login to his account with the provided password and pattern.

Step15: Stop

3.1 Flow charts:

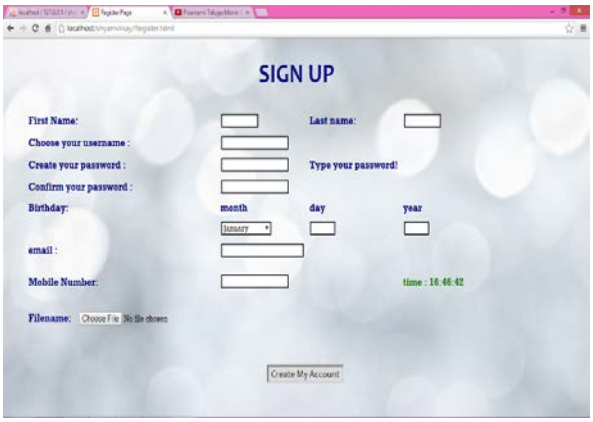
N=Name, U= Username, IP= Intervened Password, CIP=Confirm Intervened Password CP= Color Pattern, DOB=Date of Birth, M=Email Id, Ph= Phone number



4. DEMONSTRATION OF AUTHENTICATION

4.1 First Phase Registration:

Initially every user needs to sign up. In the registration page he fills the following details: First name, Last name, username, Password, Intervened Password, Date of Birth, email, mobile number.

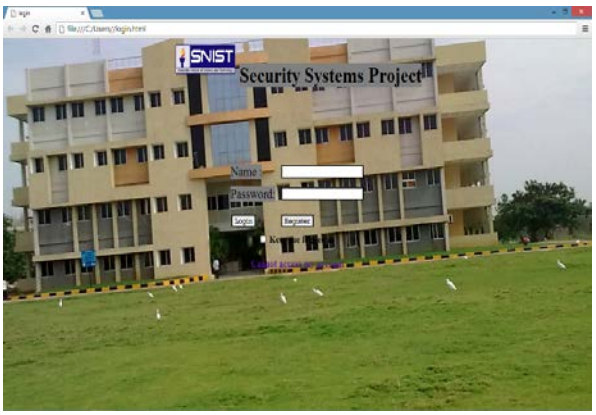


During filling in Password, user's key stroke is stored in the form of time gaps between two key strokes. During confirmation of the password, time gaps registered at the time of registration should be given. The password with these time gaps is called Intervened Password.

4.2 Second Phase Registration:

Second Phase registration consists of 4*4 color pattern where user can select a combination of minimum of 4 colors and maximum of 16 colors. For conformation the user has to re-enter the pattern which will be registered.

4.3 First Phase Login:



After registration is completed user can login to his/her account. As first factor of authentication, the user has to enter the Username and Intervened Password. The password supplied by the user with time gaps must match with the registered intervened password. For example, user has a password 'networksecurity' with a 3 seconds time gap between network and security at the time of registration. Although the intruder knew the password, he can't be authorized to the next phase because he doesn't know time gap between 'network' and 'security'.

4.4 Second Phase Login:

Fig 1

After successful in first authentication, the user needs to select his/her previously registered pattern. During this phase the layout of color pattern changes during every login, so that shoulder surfing will not be enough to authenticate unauthorized personnel. Also, user should provide the color pattern exactly in the order he/she provided during registration.

Fig 2

Let us consider user has given 'bluepinkwhitered' at the time of registration corresponding element positions are (2,1),(3,2),(2,2),(1,1). If we look at login page the colors in same sequence are at (4,1),(2,3),(1,1,),(2,2). Further, for every login attempt color pattern is produced randomly which is clearly shown in fig 2 that the layout of color pattern changed from fig 1. The first element of fig 1 is white in color whereas fig 2 is brown in color. On successful second phase authentication user redirects to home page. Therefore this

provides a more secure authentication from opponent guessing the pattern.

5. CONCLUSION

In the proposed system a new authentication system has been implemented. Compared to the existing systems it is far more secure and requires no additional hardware device for authentication. The first factor of authentication i.e. the Intervened Password is introduced to overcome the drawbacks of the traditional text password. The second factor i.e. Color pattern provides a more secure authentication which over comes the shoulder surfing. As number of elements in color pattern increases it enhances the security of the system. The color pattern cannot be interpreted by the opponent easily. The proposed system is simple, easy to implement and computationally secure against attacks.

6. REFERENCES

[1] Hardayal Singh Shekawat *"MOBILE CLOUD COMPUTING SECURITY USING TRANSIENT AUTHENTICATION SYSTEM"*, Journal of Information, Knowledge and Research in Information Technology.

[2] Anil K. Jain, Lin Hong, Sharath Pankanti *"Biometric Identificatin"*, Communications of the ACM, Volume 43, February 2000.

[3] Carl Adams, Alexandros Dimitiou *"A Two Phase Authentication Protocol Usingthe Cell Phone as a Token"*, Journal of Information Privacy and Security, Volume 4, Issue 2, 2008.

[4] Abhas Tandon, Rahul Sharma, Sankalp Sodhiya, P.M.Durai Raj Vincent *"QR Code based secure OTP distribution scheme for Authentication in Net-Banking"*, International Journal of Engineering and Technology (IJET).

Dr.Aruna Varanasi is presently working as Professor and head in the Department of Computer Science and Engineering (CSE), Sreenidhi Institute of Science and Technology (SNIST), Hyderabad, India. She was awarded "Suman Sharma" by Institute of Engineers (India), Calcutta for securing highest marks among women in India in AMIE course.

Katta Shyam Prasad is presently pursuing Bachelors of technology in Computer Science and technology from Sreenidhi Institute of Science and technology (SNIST), Hyderabad, India.

Ummaneni Vinay Kumar is presently pursuing Bachelors of technology in Computer Science and technology from Sreenidhi Institute of Science and technology (SNIST), Hyderabad, India.